

FortiWLC-SD

Command Reference



Release 8.3

March 2017

Copyright© 2016 Fortinet, Inc. All rights reserved. Fortinet® and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

Support

For assistance, contact Fortinet Customer Service and Support 24 hours a day at +1 408-542-7780, or by using one of the [local contact numbers](#), or through the Support portal at <https://support.fortinet.com/>

Fortinet Customer Service and Support provide end users and channel partners with the following:

- Technical Support
- Software Updates
- Parts replacement service

Fortinet Product License Agreement / EULA and Warranty Terms



To ensure a secured WiFi network, Fortinet hardware (controllers and access points) are designed to run only the proprietary firmware developed by Fortinet. Only approved Fortinet access points are configurable with Fortinet controllers and vice versa. Third party access points and software cannot be configured on Fortinet hardware

Trademarks and Copyright Statement

Fortinet®, FortiGate®, and FortiGuard® are registered trademarks of Fortinet, Inc., and other Fortinet names may also be trademarks, registered or otherwise, of Fortinet. All other product or company names may be trademarks of their respective owners. Copyright © 2016 Fortinet, Inc., All Rights reserved. Contents and terms are subject to change by Fortinet without prior notice. No part of this publication may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from Fortinet, Inc., as stipulated by the United States Copyright Act of 1976.

Product License Agreement

The parties to this agreement are you, the end customer, and either (i) where you have purchased your Product within the Americas, Fortinet, Inc., or (ii) where you have purchased your Product outside of the Americas, Fortinet Singapore Private Limited (each referred to herein as "Fortinet"). CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT (THE OR THIS "AGREEMENT" OR "EULA"). USE OR INSTALLATION OF FORTINET PRODUCT(S) AND ANY UPDATES THERETO, INCLUDING HARDWARE APPLIANCE PRODUCTS, SOFTWARE AND FIRMWARE INCLUDED THEREIN BY FORTINET, AND STAND-ALONE SOFTWARE PRODUCTS SOLD BY FORTINET (TOGETHER, THE "PRODUCTS") CONSTITUTES ACCEPTANCE BY YOU OF THE TERMS IN THIS AGREEMENT, AS AMENDED OR UPDATED FROM TIME TO TIME IN FORTINET'S DISCRETION BY FORTINET PUBLISHING AN AMENDED OR UPDATED VERSION. FORTINET SHALL NOT BE BOUND BY ANY ADDITIONAL AND/OR CONFLICTING PROVISIONS IN ANY ORDER, RELEASE, ACCEPTANCE OR OTHER WRITTEN CORRESPONDENCE OR OTHER WRITTEN OR VERBAL COMMUNICATION UNLESS EXPRESSLY AGREED TO IN A WRITING SIGNED BY THE GENERAL COUNSEL OF FORTINET. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, DO NOT START THE INSTALLATION PROCESS OR USE THE PRODUCTS. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, YOU SHOULD IMMEDIATELY, AND IN NO EVENT LATER THAN FIVE (5) CALENDAR DAYS AFTER YOUR RECEIPT OF THE PRODUCT IMMEDIATELY NOTIFY THE FORTINET LEGAL TEAM IN WRITING AT LEGAL@FORTINET.COM OF REQUESTED CHANGES TO THIS AGREEMENT.

1. License Grant.

This is a license, not a sales agreement, between you and Fortinet. The term "Software", as used throughout this Agreement, includes all Fortinet and third party firmware and software provided to you with, or incorporated into, Fortinet appliances and any stand-alone software provided to you by Fortinet, with the exception of any open source software contained in Fortinet's Products which is discussed in detail in section 15 below, and the term "Software" includes any accompanying documentation, any updates and enhancements of the software or firmware provided to you by Fortinet, at its option. Fortinet grants to you a non-transferable (except as provided in section 5 ("Transfer") and section 15 ("Open Source Software") below), non-exclusive, revocable (in the event of your failure to comply with these terms or in the event Fortinet is not properly paid for the applicable Product) license to use the Software solely for your internal business purposes (provided, if a substantial portion of your business is to provide managed service provider services to your end-customers, you may use the Software embedded in FortiGate and supporting hardware appliances to provide those services, subject to the other restrictions in this Agreement), in accordance with the terms set forth in this Agreement and subject to any further restrictions in Fortinet documentation, and solely on the Fortinet appliance, or, in the case of blades, CPUs or databases, on the single blade, CPU or database on which Fortinet installed the Software or, for stand-alone Software, solely on a single computer running a validly licensed copy of the operating system for which the Software was designed, or, in the case of blades, CPUs or databases, on a single blade, CPU or database. For clarity, notwithstanding anything to the contrary, all licenses of Software to be installed on blades, CPUs or databases are licensed on a per single blade, solely for one blade and not for multiple blades that may be installed in a chassis, per single CPU or per single database basis, as applicable. The Software is "in use" on any Fortinet appliances when it is loaded into temporary memory (i.e. RAM). You agree that, except for the limited, specific license rights granted in this section 1, you receive no license rights to the Software.

2. Limitation on Use.

You may not attempt to, and, if you are a corporation, you are responsible to prevent your employees and contractors from attempting to, (a) modify, translate, reverse engineer, decompile, disassemble, create derivative works based on, sublicense, or distribute the Software; (b) rent or lease any rights in the Software in any form to any third party or make the Software available or accessible to third parties in any other manner; (c) except as provided in section 5, transfer assign or sublicense right to any other person or entity, or (d) remove any proprietary notice, labels, or marks on the Software, Products, and containers.

3. Proprietary Rights.

All rights, title, interest, and all copyrights to the Software and any copy made thereof by you and to any Product remain with Fortinet. You acknowledge that no title to the intellectual property in the Software or other Products is transferred to you and you will not acquire any rights to the Software or other Products except for the specific license as expressly set forth in section 1 ("License Grant") above. You agree to keep confidential all Fortinet

confidential information and only to use such information for the purposes for which Fortinet disclosed it.

4. Term and Termination.

Except for evaluation and beta licenses or other licenses where the term of the license is limited per the evaluation/beta or other agreement or in the ordering documents, the term of the license is for the duration of Fortinet's copyright in the Software. Fortinet may terminate this Agreement, and the licenses and other rights herein, immediately without notice if you breach or fail to comply with any of the terms and conditions of this Agreement. You agree that, upon such termination, you will cease using the Software and any Product and either destroy all copies of the Fortinet documentation or return all materials to Fortinet. The provisions of this Agreement, other than the license granted in section 1 ("License Grant"), shall survive termination.

5. Transfer.

If you are a Fortinet contracted and authorized reseller or distributor of Products, you may transfer (not rent or lease unless specifically agreed to in writing by Fortinet) the Software to one end user on a permanent basis, provided that: (i) you ensure that your customer and the end user receives a copy of this Agreement, is bound by its terms and conditions, and, by selling the Product or Software, you hereby agree to enforce the terms in this Agreement against such end user, (ii) you at all times comply with all applicable United States export control laws and regulations, and (iii) you agree to refund any fees paid to you by an end user who purchased Product(s) from you but does not agree to the terms contained in this Agreement and therefore wishes to return the Product(s) as provided for in this Agreement. Further, if you are a non-authorized reseller of Products, you are not authorized to sell Product(s) or Software, but, regardless, by selling Product(s) or Software, you hereby agree you are bound by the restrictions and obligations herein and are bound to: (i) ensure that your customer and the end user receive a copy of this Agreement and are bound in full by all restrictions and obligations herein (ii) enforce the restrictions and obligations in this Agreement against such customer and/or end user, (iii) comply with all applicable United States export control laws and regulations and all other applicable laws, and (iv) refund any fees paid to you by a customer and/or end user who purchased Product(s) from you but does not agree to the restrictions and obligations contained in this Agreement and therefore wishes to return the Product(s) as provided for in this Agreement. Notwithstanding anything to the contrary, distributors, resellers and other Fortinet partners (a) are not agents of Fortinet and (b) are not authorized to bind Fortinet in any way.

6. Limited Warranty.

Fortinet provides this limited warranty for its product only to the single end-user person or entity that originally purchased the Product from Fortinet or its authorized reseller or distributor and paid for such Product. The warranty is only valid for Products which are properly registered on Fortinet's Support Website, <https://support.fortinet.com>, or such other website as provided by Fortinet, or for which the warranty otherwise

starts according to Fortinet's policies. The warranty periods discussed below will start according to Fortinet's policies posted at <http://www.fortinet.com/aboutus/legal.html> or such other website as provided by Fortinet. It is the Fortinet distributor's and reseller's responsibility to make clear to the end user the date the product was originally shipped from Fortinet, and it is the end user's responsibility to understand the original ship date from the party from which the end user purchased the product. All warranty claims must be submitted in writing to Fortinet before the expiration of the warranty term or such claims are waived in full. Fortinet provides no warranty for any beta, donation or evaluation Products, for any spare parts not purchased directly from Fortinet by the end-user, for any accessories, or for any stand-alone software. Fortinet warrants that the hardware portion of the Products, including spare parts unless noted otherwise ("Hardware") will be free from material defects in workmanship as compared to the functional specifications for the period set forth as follows and applicable to the Product type ("Hardware Warranty Period"): a three hundred sixty-five (365) day limited warranty for the Hardware excluding spare parts, power supplies, and accessories (provided, solely with respect to FortiAP and Meru AP indoor Wi-Fi access point Hardware appliance products and FortiSwitch Hardware appliance products other than the FortiSwitch-5000 series (for both excluding spare parts, power supplies, and accessories), the warranty herein shall last from the start of the warranty period as discussed above until five (5) years following the product announced end-of-life date), and, for spare parts, power supplies, and accessories, solely a ninety (90) days limited warranty. Fortinet's sole obligation shall be to repair or offer replacement Hardware for the defective Hardware at no charge to the original owner. This obligation is exclusive of transport fees, labor, de-installation, installation, reconfiguration, or return shipment and handling fees and costs, and Fortinet shall have no obligation related thereto. Such repair or replacement will be rendered by Fortinet at an authorized Fortinet service facility as determined by Fortinet. The replacement Hardware need not be new or of an identical make, model, or part; Fortinet may, in its discretion, replace the defective Hardware (or any part thereof) with any reconditioned Product that Fortinet reasonably determines is substantially equivalent (or superior) in all material respects to the defective Hardware. The Hardware Warranty Period for the repaired or replacement Hardware shall be for the greater of the remaining Hardware Warranty Period or ninety days from the delivery of the repaired or replacement Hardware. If Fortinet determines in its reasonable discretion that a material defect is incapable of correction or that it is not practical to repair or replace defective Hardware, the price paid by the original purchaser for the defective Hardware will be refunded by Fortinet upon return to Fortinet of the defective Hardware. All Hardware (or part thereof) that is replaced by Fortinet, or for which the purchase price is refunded, shall become the property of Fortinet upon replacement or refund. Fortinet warrants that the software as initially shipped with the Hardware Products will substantially conform to Fortinet's then current functional specifications for the Software, as set forth in the applicable documentation for a period of ninety (90) days ("Software Warranty Period"), if the Software is properly installed on approved Hardware and operated as contemplated in its documentation. Fortinet's sole obligation shall be to repair or offer replacement Software for the non-conforming Software with software that substantially conforms to Fortinet's functional specifications. This obligation is exclusive of transport fees, labor, de-installation, installation, reconfiguration, or return shipment and handling fees and costs, and Fortinet shall have no obligation related thereto. Except as otherwise agreed by

Fortinet in writing, the warranty replacement Software is provided only to the original licensee, and is subject to the terms and conditions of the license granted by Fortinet for the Software. The Software Warranty Period shall extend for an additional ninety (90) days after any warranty replacement software is delivered. If Fortinet determines in its reasonable discretion that a material non-conformance is incapable of correction or that it is not practical to repair or replace the non-conforming Software, the price paid by the original licensee for the non-conforming Software will be refunded by Fortinet; provided that the non-conforming Software (and all copies thereof) is first returned to Fortinet. The license granted respecting any Software for which a refund is given automatically terminates immediately upon refund. For purpose of the above hardware and software warranties, the term "functional specifications" means solely those specifications authorized and published by Fortinet that expressly state in such specifications that they are the functional specifications referred to in this section 6 of this Agreement, and, in the event no such specifications are provided to you with the Software or Hardware, there shall be no warranty on such Software.

7. Disclaimer of Other Warranties and Restrictions.

EXCEPT FOR THE LIMITED WARRANTY SPECIFIED IN SECTION 6 ABOVE, THE PRODUCT AND SOFTWARE ARE PROVIDED "AS-IS" WITHOUT ANY WARRANTY OF ANY KIND INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY, IMPLIED OR EXPRESS WARRANTY OF MERCHANTABILITY, OR WARRANTY FOR FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. IF ANY IMPLIED WARRANTY CANNOT BE DISCLAIMED IN ANY TERRITORY WHERE A PRODUCT IS SOLD, THE DURATION OF SUCH IMPLIED WARRANTY SHALL BE LIMITED TO NINETY (90) DAYS FROM THE DATE OF ORIGINAL SHIPMENT FROM FORTINET. EXCEPT AS EXPRESSLY COVERED UNDER THE LIMITED WARRANTY PROVIDED HEREIN, THE ENTIRE RISK AS TO THE QUALITY, SELECTION AND PERFORMANCE OF THE PRODUCT IS WITH THE PURCHASER OF THE PRODUCT. NOTWITHSTANDING ANYTHING TO THE CONTRARY, THE HARDWARE WARRANTY PERIOD DISCUSSED ABOVE DOES NOT APPLY TO CERTAIN FORTINET PRODUCTS, INCLUDING FORTITOKEN WHICH HAS A 365 DAY WARRANTY FROM THE DATE OF SHIPMENT FROM FORTINET'S FACILITIES, AND THE SOFTWARE WARRANTY DOES NOT APPLY TO CERTAIN FORTINET PRODUCTS, INCLUDING FORTIGATE-ONE AND VDOM SOFTWARE. YOU HEREBY ACKNOWLEDGE AND AGREE THAT NO VENDOR CAN ASSURE COMPLETE SECURITY AND NOTHING HEREIN OR ELSEWHERE SHALL BE DEEMED TO IMPLY A SECURITY GUARANTEE OR ASSURANCE. The warranty in Section 6 above does not apply if the Software, Product or any other equipment upon which the Software is authorized to be used (a) has been altered, except by Fortinet or its authorized representative, (b) has not been installed, operated, repaired, updated to the latest version, or maintained in accordance with instructions supplied by Fortinet, (c) has been subjected to abnormal physical or electrical stress, misuse, negligence, or accident; (d) is licensed for beta, evaluation, donation, testing or demonstration purposes or for which Fortinet does not charge a purchase price or license fee. In the case of beta, testing, evaluation, donation or free Software or Product, the end user acknowledges and agrees that such Software or Product may contain bugs or

errors and could cause system failures, data loss and other issues, and the end user agrees that such Software or Product is provided “as-is” without any warranty whatsoever, and Fortinet disclaims any warranty or liability whatsoever. An end user’s use of evaluation or beta Software or Product is limited to thirty (30) days from original shipment unless otherwise agreed in writing by Fortinet.

8. Governing Law.

Any disputes arising out of this Agreement or Fortinet’s limited warranty shall be governed by the laws of the state of California, without regard to the conflict of laws principles. In the event of any disputes arising out of this Agreement or Fortinet’s limited warranty, the parties submit to the jurisdiction of the federal and state courts located in Santa Clara County, California, as applicable.

9. Limitation of Liability.

TO THE MAXIMUM EXTENT PERMITTED BY LAW AND NOTWITHSTANDING ANYTHING TO THE CONTRARY, FORTINET IS NOT LIABLE UNDER ANY CONTRACT, NEGLIGENCE, TORT, STRICT LIABILITY, INFRINGEMENT OR OTHER LEGAL OR EQUITABLE THEORY FOR ANY LOSS OF USE OF THE PRODUCT OR SERVICE OR ANY DAMAGES OF ANY KIND WHATSOEVER, WHETHER DIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF GOODWILL, LOSS OF PROFIT, LOSS OF OPPORTUNITY, LOSS OR DAMAGE RELATED TO USE OF THE PRODUCT OR SERVICE IN CONNECTION WITH HIGH RISK ACTIVITIES, DE-INSTALLATION AND INSTALLATION FEES AND COSTS, DAMAGE TO PERSONAL OR REAL PROPERTY, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, COMPUTER SECURITY BREACH, COMPUTER VIRUS INFECTION, LOSS OF INFORMATION OR DATA CONTAINED IN, STORED ON, OR INTEGRATED WITH ANY PRODUCT INCLUDING ANY PRODUCT RETURNED TO FORTINET FOR WARRANTY SERVICE) RESULTING FROM THE USE OF THE PRODUCT, RELATING TO WARRANTY SERVICE, OR ARISING OUT OF ANY BREACH OF THE LIMITED WARRANTY IN SECTION 6 ABOVE, EVEN IF FORTINET HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE SOLE REMEDY FOR A BREACH OF THE LIMITED WARRANTY IS REPAIR, REPLACEMENT OR REFUND OF THE DEFECTIVE OR NONCONFORMING PRODUCT AS SPECIFICALLY STATED IN SECTION 6 ABOVE.

10. Import / Export Requirements; FCPA Compliance.

You are advised that the Products may be subject to the United States Export Administration Regulations and other import and export laws; diversion contrary to United States law and regulation is prohibited. You agree to comply with all applicable international and national laws that apply to the Products as well as end user, end-use, and destination restrictions issued by U.S. and other governments. For additional information on U.S. export controls see www.bis.doc.gov. Fortinet assumes no responsibility or liability for your failure to obtain any

necessary import and export approvals, and Fortinet reserves the right to terminate or suspend shipments, services and support in the event Fortinet has a reasonable basis to suspect any import or export violation. You represent that neither the United States Bureau of Industry and Security nor any other governmental agency has issued sanctions against you or otherwise suspended, revoked or denied your export privileges. You agree not to use or transfer the Products for any use relating to nuclear, chemical or biological weapons, or missile technology, unless authorized by the United States Government by regulation or specific written license. Additionally, you agree not to directly or indirectly export, import or transmit the Products contrary to the laws or regulations of any other governmental entity that has jurisdiction over such export, import, transmission or use. Furthermore, you represent that you understand, and you hereby agree to comply with, all requirements of the U.S. Foreign Corrupt Practices Act and all other applicable laws. For beta, testing, evaluation, donation or free Products and/or related services, you hereby agree, represent and warrant to Fortinet that (a) receipt of the Products and/or services comply with all policies and you have obtained all necessary approvals for such Products and/or services, (b) the Products and/or services are not provided in exchange for Fortinet maintaining current business or for new business opportunities, and (c) the Products and/or services are not being received for the benefit of, and are not being transferred to, any government entity, representative or affiliate.

11. U.S. Government End Users.

The Software and accompanying documentation are deemed to be "commercial computer software" and "commercial computer software documentation," respectively, pursuant to DFAR Section 227.7202 and FAR Section 12.212, as applicable. Any use, modification, reproduction, release, performance, display or disclosure of the Software and accompanying documentation by the United States Government shall be governed solely by the terms of this Agreement and shall be prohibited except to the extent expressly permitted by the terms of this Agreement and its successors.

12. Tax Liability.

You agree to be responsible for payment of any sales or use taxes imposed at any time on this transaction.

13. General Provisions.

Except as specifically permitted and required in section 5 ("Transfer") above, you agree not to assign this Agreement or transfer any of the rights or obligations under this Agreement without the prior written consent of Fortinet. This Agreement shall be binding upon, and inure to the benefit of, the successors and permitted assigns of the parties. The United Nations Convention on Contracts for the International Sales of Goods is expressly excluded. This Agreement and other Fortinet agreements may be amended or supplemented only by a writing that refers explicitly to the agreement signed on behalf of both parties, or, for this Agreement, as otherwise expressly provided in the lead-in above Section 1 above, provided, notwithstanding anything to the contrary and except for this Agreement which may be amended or updated as expressly provided in the lead-in above Section 1 above, for any amendment or other agree-

ment to be binding on Fortinet, such amendment or other agreement must be signed by Fortinet's General Counsel. No waiver will be implied from conduct or failure to enforce rights nor effective unless in a writing signed on behalf of the party against whom the waiver is asserted. If any part of this Agreement is found unenforceable, that part will be enforced to the maximum extent permitted and the remainder shall continue in full force and effect. You acknowledge that you have read this Agreement, understand it, and agree to be bound by its terms and conditions.

14. Privacy.

For information regarding Fortinet's collection, use and transfer of your personal information please read the Fortinet privacy policy on the Fortinet web site (<http://www.fortinet.com/aboutus/privacy.html>).

15. Open Source Software.

Fortinet's products may include software modules that are licensed (or sublicensed) to the user under the GNU General Public License, Version 2, of June 1991 ("GPL") or GNU Lesser General Public License, Version 2.1, of February 1999 ("LGPL") or other open source software licenses which, among other rights, permit the user to use, copy, modify and redistribute modules, or portions thereof, and may also require attribution disclosures and access to the source code ("Open Source Software"). The GPL requires that for any Open Source Software covered under the GPL, which is distributed to someone in an executable binary format, that the source code also be made available to those users. For any Open Source Software covered under the GPL, the source code is made available on this CD or download package. If any Open Source Software licenses require that Fortinet provide rights to use, copy or modify a Open Source Software program that are broader than the rights granted in this agreement, then such rights shall take precedence over the rights and restrictions herein. Fortinet will provide, for a charge reflecting our standard distribution costs, the complete machine-readable copy of the modified software modules. To obtain a complete machine-readable copy, please send your written request, along with a check in the amount of US \$25.00, to General Public License Source Code Request, Fortinet, Inc., 899 Kifer Rd, Sunnyvale, CA 94086 USA. In order to receive the modified software modules, you must also include the following information: (a) Name, (b) Address, (c) Telephone number, (d) E-mail Address, (e) Product purchased (if applicable), (f) Product Serial Number (if applicable). All open source software modules are licensed free of charge. There is no warranty for these modules, to the extent permitted by applicable law. The copyright holders provide these software modules "AS-IS" without warranty of any kind, either expressed or implied. In no event will the copyright holder for the open source software be liable to you for damages, including any special, incidental or consequential damages arising out of the use or inability to use the software modules, even if such holder has been advised of the possibility of such damages. A full copy of this license, including additional open source software license disclosures and third party license disclosures applicable to certain Fortinet products, may be obtained by contacting Fortinet's Legal Department at legal@fortinet.com.

GNU GENERAL PUBLIC LICENSE GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you". Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the

Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program. You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if

the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.) These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.. Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program. In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

Source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable. If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under

this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

GNU LESSER GENERAL PUBLIC LICENSE

Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.

59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library. You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

- a) The modified work must itself be a software library.
- b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.
- c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.
- d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it. Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library. In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2 instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy. This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not.

Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.) Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for your own use and reverse engineering for debugging such modifications. You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of

definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy. For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable. It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this

License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice. This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. Each version is

given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

15. The warranty disclaimer contained in Sections 11 and 12 of the preceding GPL License is incorporated herein.

Table of Contents

Support	ii
About This Guide.	37
Audience	37
Related Publications	38
External References	38
Guide to Typographic Conventions	38
Syntax Notation	39
Contacting Fortinet	40
Key Concepts	41
Getting Started	41
CLI Command Modes	42
User EXEC Mode	42
Privileged EXEC Mode	42
Global Configuration Mode	43
Command Line-Only Commands	43
Abbreviating Commands	45
Using No and Default Forms of Commands	46
Getting Help.	47
Using Command History	48
Setting the Command History Buffer Size.	48
Recalling Commands	49

Disabling the Command History Feature	49
Finding Words in show Command Output.	49
Customizing the CLI Prompt	50
Default CLI Prompt	50
Commands to Customize CLI Prompt.	50
Manipulating Terminal Characteristics	50
Displaying Terminal Settings.	50
Setting Terminal Screen Length and Width	50
Ending a Session.	51
Password Spacing.	51
User Interface Commands	53
?	54
disable	55
do	56
enable	57
end	58
exit	59
help	60
prompt	62
quit	63
show history.	64
show terminal	65
terminal history	66
terminal history size.	67

terminal length	68
terminal width	69
File Management Commands	71
cd	72
copy	73
copy running-config	75
delete	77
dir	79
downgrade	81
more	82
pwd	84
rename	85
run	86
show controller file systems	87
show flash	89
show running-config	90
show startup-config	91
show scripts	92
upgrade ap	93
upgrade controller	95
upgrade system	97
patch upgrade	99
System Management Commands	103
10gig-module	106

aeroscout	107
alarm	108
amconfig	111
audit period	112
bonding	113
calendar set	115
clear statistics interfaces	117
client-locator	118
controller-index	120
date	121
erase-guest-user	122
event	123
fastpath	126
fingerprint	127
guest-user	128
hostname	130
ip udp-broadcast downstream	131
ip udp-broadcast downstream-bridged	132
ip udp-broadcast upstream	133
ip udp-broadcast upstream-bridged	134
license	135
management wireless	137
nms-profile	138
nms-server	139

nms-vpn-server	140
ntp	141
passwd	142
ping	143
poweroff controller	144
proactive-spectrum-manager	145
proxy-arp-filtering	148
reload	149
reload-gui	151
reload-management	152
reload-security	153
reload-snmp	154
reload-vpn	155
reload-wapi	156
remove-license	157
roaming-domain	158
setup	161
show alarm	163
show ap-neighbor	165
show bonding	169
show calendar	171
show client-locator	172
show controller	173
show controller cpu-utilization	177

show controller file systems	178
show controller memory	180
show controller processes	182
show controller mobility-vars	184
show event	185
show fastpath	187
show features	189
show fingerprints	190
show flash	191
show guest-user	192
show interfaces accel	193
show hostname	194
show license	195
show ip udp-broadcast downstream all-ports	197
show ip udp-broadcast downstream-bridged all-ports	198
show ip udp-broadcast upstream all-ports	199
show ip udp-broadcast upstream-bridged all-ports	200
show license-file	201
show log	202
show nms-server	203
show ntp-server	204
show roaming-domain	205
show syslog-file	207
show syslog-host	209

show syslog-table	210
show sys-summary	212
show sys-summary ess	214
show sys-summary general	216
show sys-summary resources	218
show sys-summary stations	219
show sys-summary throughput	220
show system-id	221
show timezones	222
spectrum-band	223
start-ntp	224
statistics period	225
Sysconfig backup	226
Sysconfig restore	227
syslog-host	228
telnet	229
timezone	230
topo-update	233
traceroute	234
zeronet-packet	235
Redundancy Commands	237
nplus1 add	238
nplus1 delete	240
nplus1 disable	241

nplus1 enable	242
nplus1 period	243
nplus1 revert	244
nplus1 autorevert	245
nplus1 setdebugloglevel	246
nplus1 start master	247
nplus1 start slave	248
nplus1 stop	250
nplus1 takeover	251
nplus1 timeout	252
show nplus1	253
show nplus1 debugloglevel	257
Interface and IP Commands	259
gw	261
igmp-snoop	262
interface FastEthernet	264
ip address	266
ip address dhcp	268
ip default-gateway	269
ip dhcp-passthrough	271
ip dhcp-server	272
ip dns-server	273
ip domainname	274
ip ftp	275

ip scp	276
ip sftp	277
ip udp-broadcast	278
ipv6-neighbor-discovery-optimization	280
mac-address	281
port-profile	282
(config-port-profile) ap-vlan-tag	283
(config-port-profile) dataplane	284
(config-port-profile) disable	285
(config-port-profile) enable	286
(config-port-profile) multicast-enable	287
(config-port-profile) show	288
(config-port-profile) vlan	289
(config-port-profile) ip-prefix-validation-enable	290
show igmp-snoop	292
show interfaces FastEthernet ap	294
show interfaces FastEthernet controller	297
show interfaces FastEthernet statistics	300
show ip	302
show ipv6-neighbor	304
show second_interface_status	305
static-route	306
(config-static-route) interface	307
(config-static-route) ip	308

type	309
virtual-interface-profile	311
(config-vip) disable	312
(config-vip) enable	313
(config-vip) gateway	314
(config-vip) ip	315
(config-vip) show	316
VLAN Commands	317
dhcp-server	319
(config-dhcp-server) disable	321
(config-dhcp-server) dns-server-primary	322
(config-dhcp-server) dns-server-secondary	323
(config-dhcp-server) domain-name	325
(config-dhcp-server) enable	326
(config-dhcp-server) ip-pool	327
(config-dhcp-server) lease-time	329
(config-dhcp-server) netbios-server-primary	331
(config-dhcp-server) netbios-server-secondary	333
(config-dhcp-server) option-43	335
(config-dhcp-server) show	337
(config-dhcp-server) vlan	338
(config-dhcp-server) virtual-interface-profile	340
gre	342
interface FastEthernet controller	344

ip remote-external-address	346
ip tunnel-ip-address	347
show dhcp-server	348
show gre	350
show dhcp-lease	351
show vlan.	352
test gre.	354
vlan	355
wapi-server	356
Security Commands	357
8021x-network-initiation.	361
802.1x-termination.	362
access-list deny	363
access-list deny import	365
access-list permit.	367
access-list permit import	369
mac-filter-state.	371
administrator guest	372
allowed-l2-modes	373
app-visibility-policy	375
app-visibility-custom-application	377
sh service-summary Application-Visibility	378
authentication-mode	380
authentication-mode global	382

authentication-type	384
captive-portal	388
captive-portal-auth-method	390
cef	392
certmgmt delete-ca	395
certmgmt delete-csr	397
certmgmt delete-server	398
certmgmt export-ca	400
certmgmt export-csr	402
certmgmt export-server	404
certmgmt list-ca	406
certmgmt list-csr	408
certmgmt list-server	409
certmgmt view-ca	411
certmgmt view-csr	413
certmgmt view-server	414
change_mac_state	416
clear certificates	418
description	419
encryption-modes ccmp	420
encryption-modes ccmp-tkip	421
encryption-modes tkip	422
encryption-modes wep128	423
encryption-modes wep64	424

firewall-capability	425
firewall-filter-id	426
firewall-filter-id-flow	427
group-rekey interval	428
import	429
ip-address	430
key	431
key-rotation	432
local-admin	433
mac-delimiter	435
macfiltering	436
password	437
password-type	439
PMK-caching	440
pmk caching	441
port	442
primary-tacacs-ip	443
primary-tacacs-port	445
primary-tacacs-secret	447
privilege-level	449
psk key	452
radius-profile	454
radius-server primary	456
radius-server secondary	457

reauth	458
rekey period.	459
secondary-tacacs-ip	460
secondary-tacacs-port.	462
secondary-tacacs-secret	464
security-logging	466
security-profile	467
shared-authentication	470
show aaa statistics	472
show access-list deny	473
show access-list permit	474
show air-shield.	475
show arp	476
show authentication-mode.	478
show cef	479
show local-admins.	480
show radius-profile	482
show security-profile	484
show ssl-server	487
show web.	488
ssl-server accounting-radius-profile.	490
ssl-server associate.	492
ssl-server captive-portal	493
ssl-server captive-portal-external_URL	495

ssl-server port	497
ssl-server radius-profile	498
ssl-server cna-bypass	499
static-wep key	501
static-wep key-index	503
tunnel-termination	504
vpn client	505
(config-vpn-client) vpn-client-state.	506
(config-vpn-client) vpn-server-ip	507
(config-vpn-client) vpn-server-port.	508
vpn server	509
(config-vpn) encryption	510
(config-vpn) ip-pool	511
(config-vpn) port	512
(config-vpn) subnet-mask	513
(config-vpn) vpn-server-ip	514
(config-vpn) vpn-server-state.	515
web custom	516
web login-page	518
ESSID Commands	519
accounting interim-interval.	521
accounting primary-radius	522
accounting secondary-radius.	524
ap-discovery join-ess.	526

ap-discovery join-virtual-ap	527
ap-vlan priority	529
ap-vlan-tag.	530
apsd	531
band-steering-mode	533
band-steering-timeout	534
base-tx-rates	536
beacon dtim-period	538
beacon period	539
bssid	540
calls-per-bss	541
countermeasure.	542
dataplane.	543
edited-bssid	545
ess-ap	546
essid	547
gre name	548
l2bridge airf	549
l2bridge appletalk	550
l2bridge ipv6	551
multicast-enable	552
multicast-mac-transparency	553
overflowfrom-essprofile	554
publish-essid	556

security-profile	557
show ess-ap	558
show edited-bssid	559
show essid	560
ssid	563
supported-tx-rates	564
tunnel-type	566
virtual-port	567
vlan name	568
wireless-to-wireless-isolation	569
Access Point and Radio Commands	571
admin-mode	574
antenna-gain	575
antenna-property	576
antenna-selection	577
ap	578
ap-keepalive-timeout	580
ap-redirect	581
auto-ap-upgrade	582
autochannel	584
boot-script	585
building	586
channel	587
channel-width	589

connectivity	590
contact	592
controller domainname	593
controller hostname	594
controller ip	595
dataplane-encryption	596
description	597
fixed-channel	598
floor	599
hostname	600
interface Dot11Radio	601
led	603
link	604
link-probing-duration	605
keepalive-timeout	606
localpower	607
location	609
mac-address	610
mimo-mode	611
mode	613
model	614
n-only-mode	615
parent-ap	616
power-supply	618

preamble-short	620
protection-cts-mode	621
protection-mode	622
rfband	623
rf-mode	624
role	625
show ap	627
show ap-connectivity	630
show ap-discovered	632
show ap-redirect	634
show ap-swap	635
show ess-ap	636
show interfaces Dot11Radio	637
show interfaces Dot11Radio antenna-property	639
show interfaces Dot11Radio statistics	642
show regulatory-domain	647
show statistics ap300-diagnostics	648
show statistics station-per-ap	650
show statistics top10-ap-problem	651
show statistics top10-ap-talker	653
show topoap	655
show topoapap	656
swap ap	658
type	661

Mesh Commands	663
admin-mode.	664
descr	665
mesh-ap.	666
mesh-profile.	667
plugnplay	668
psk	669
Rogue AP Detection Commands	671
rogue-ap acl.	672
rogue-ap aging	673
rogue-ap assigned-aps	674
rogue-ap blocked.	675
rogue-ap detection.	677
rogue-ap min-rssi.	678
rogue-ap mitigation	679
rogue-ap mitigation-frames	680
rogue-ap operational-time	681
rogue-ap scanning-channels	682
rogue-ap scanning-time.	684
show rogue-ap acl	685
show rogue-ap blocked	686
show rogue-ap globals	687
show rogue-ap-list	688
Quality-of-Service Commands	689

action	691
avgpacketrates	692
dscp	693
dstip	694
dstip-flow	695
dstip-match	696
dstmask	697
dstport	698
dstport-flow	700
dstport-match.	701
firewall-filter-id	702
firewall-filter-id-flow	704
firewall-filter-id-match	706
netprotocol-flow	708
netprotocol-match	709
packet max-length	710
packet min-length	711
packet-min-length-flow	712
packet-min-length-match	713
peakrate.	714
priority	715

qoscodec	716
qosrule	719
qosrule-logging-frequency	722
qosrulelogging	723
qosvars admission	724
qosvars bwscaling	726
qosvars cac-deauth	727
qosvars calls-per-ap	728
qosvars calls-per-bssid	729
qosvars calls-per-interference	730
qosvars drop-policy	731
qosvars enable	732
qosvars intercell-periodicity	734
qosvars load-balance-overflow	735
qosvars max-stations-per-radio	736
qosvars max-stations-per-bssid	737
qosvars sip-idle-timeout	738
qosvars station-assign-age	739
qosvars tcpttl	740
qosvars ttl	741
qosvars udpttl	742
rspeccrate	743
rspecslack	744
srcip	745

srcmask	746
srcport	747
show phones	749
show phone-calls	750
show qoscodec	751
show qosflows	754
show qosrule	756
show qosstats	761
show qosvars	762
show statistics call-admission-control	764
tokenbucketrate	766
tokenbucketsize	768
trafficcontrol-enable	769
SNMP Commands	771
reload-snmp	772
show snmp-community	773
show snmp-trap	774
show snmpv3-user	775
snmp-filter-config	776
snmpv3-user	777
snmpv3-user auth-key	778

snmpv3-user auth-protocol	779
snmpv3-user priv-key	780
snmpv3-user priv-protocol	781
snmpv3-user target ip-address	782
snmp start and snmp stop	783
snmp-server community	784
snmp-server contact	785
snmp-server description	786
snmp-server location	787
snmp-server trap	788
show snmp-filter-config	789
Station Commands	791
associated-station-max-idle-period	793
no station	794
show ap-assigned	795
show dot11 associations	797
show dot11 statistics client-traffic	799
show static-station	802
show station-log-config	803
show station commands	805
show station	807
show station 802.11	809
show station all	811
show station counter	813

show station details	815
show station general	819
show station mac-address	822
show station multiple-ip	824
show station network	825
show station security	828
show statistics station-per-ap	831
show statistics top10-station-problem	833
show statistics top10-station-talker	835
show topostaap	837
show topostation	838
static-station	840
station-aging-out-interval	841
station-log	843
(station-log) enable	846
(station-log) filelog	847
(station-log) syslog	848
(station-log) event id	849
(station-log) event severity	851
(station-log) show filters	853
station-log show	855

Service Control Commands	857
blocked-gateway	858
policy	859
service-type	861
service-control-config active-discovery	862
service-control-config essids	863
service-control-config gateways	864
service-control-config locations	865
service-control-config service-types	866
service-control-config state	867
service-control-config vlans	868
show service-control blocked-gateway	869
show service-control global-config	870
show service-control global-config-service	871
show service-control global-discovered-service	872
show service-control global-discovered-service-summary	873
show service-control location	874
show service-control policy	875
show service-control policy-config-service	876
show service-control policy-service	877
show service-control policy-service-summary	878
show service-control service-type	879
show service-control user-group	880
user-group	881

Troubleshooting Commands 883

analyze-capture	885
auto-report admin	886
auto-report send	888
capture-packets	890
debug captive-portal	897
debug connect	898
debug controller	899
debug eap	900
debug mac-filter	901
debug module	902
(diag-log) admin	906
(diag-log) config	908
(diag-log) restore	910
diagnostics	912
diagnostics-ap	914
diagnostics-controller	916
packet-capture-profile	918
(packet capture profile) ap-list	921
(packet capture profile) capture-sibling-frames	923
(packet-capture-profile) enable-profile	930

(packet capture profile) filter	932
(packet capture profile) interface list	933
(packet capture profile) mode	934
(packet capture profile) packet-truncation-length	936
(packet capture profile) rate-limiting	937
(packet capture profile) rate-limiting-mode	939
(packet capture profile) rxtx	940
(packet capture profile) token-bucket-rate	942
(packet capture profile) token-bucket-size	945
remote-log	948
show auto-report-config	949
show cef	951
show debug	952
show diag-log-config ap/controller/station	953
show packet-capture-profile	959
show statistics AP300-diagnostics	961

1 About This Guide

This guide provides a detailed description of FortiWLC (SD) commands that are executed at the Fortinet Controller Command Line Interface (CLI). Each chapter of this reference contains a list of related commands, such as commands that are used to manage APs or configure system security. At the end of the guide is an alphabetical listing of all commands that are contained within the FortiWLC (SD). Clicking a command's page number in that listing will take you to the command entry.

Use this book as a reference for individual commands. To understand how the various commands are used together to accomplish system tasks such as setting up system security for a wireless LAN or configuring an ESSID, refer to the companion guide, the FortiWLC (SD) Configuration Guide. There you will find a chapter structure that mirrors that of this book, with background reference information, detailed explanations, and procedures for performing system configuration and maintenance tasks.



Features or options not documented in this guide are not supported.

Audience

This guide is intended for network administrators configuring and maintaining the Wireless LAN System. Familiarity with the following concepts is helpful when configuring the Fortinet Wireless LAN System:

- Network administration, including:
 - Internet Protocol (IP) addressing and routing
 - Dynamic Host Configuration Protocol (DHCP)
 - Configuring Layer 2 and Layer 3 switches (if required by your switch)
- IEEE 802.11 (Wi-Fi) concepts, including:
 - ESSIDs
 - WEP

- Network Security (optional)
 - WPA
 - 802.1X
 - RADIUS
 - X.509 certificates

Related Publications

- *FortiWLC-SD Release Notes*
- *FortiWLC-SD Configuration Guide*

External References

- Stevens, W. R. 1994. *TCP/IP Illustrated, Volume 1, The Protocols*. Addison-Wesley, Reading, Mass.
- Gast, M.S. 2002. *802.11 Wireless Networks, The Definitive Guide*. O'Reilly and Associates, Sebastopol, Calif.

Guide to Typographic Conventions

This guide uses the following typographic conventions in paragraph text to help you identify information:

Bold text	Identifies commands and keywords in syntax descriptions that are entered literally.
<i>Italic text</i>	Used for new terms, emphasis, and book titles; also identifies arguments for which you supply values in syntax descriptions.
Courier font	Identifies file names, folder names, computer screen output, and text in syntax descriptions that you are required to type.
help	Denotes a cross-reference link to a command. Clicking the link takes you to the command reference entry.
Ctrl-	Denotes that the Ctrl key should be used in conjunction with another key, for example, Ctrl-D means hold down the Ctrl and press the D key. Keys are shown in capitals, but are not case sensitive.



Provides extra information, tips, and hints regarding the topic



Identifies important information about actions that could result in damage to or loss of data, or could cause the application to behave in unexpected ways.



Identifies critical information about actions that could result in equipment failure or bodily harm.

Syntax Notation

In example command syntax descriptions and examples, the following text elements and punctuation are used to denote user input and computer output for the command.

bold	Required command, keywords, and punctuation.
<i>italic</i>	Arguments or file names where you substitute a value.
no	The optional no form of the command disables the feature or function.
[]	Optional elements are enclosed by square brackets.
{ }	Braces indicates that one of the enclosed elements must be used.
	Choices among elements are separated by vertical bars.
[{}]	A required choice within an optional element.
...	The preceding argument can be repeated.

The following figure shows a sample of syntax notation.

[no] action target {keyword|keyword} [argument ...]

Diagram illustrating the syntax notation components:

- The optional **no** form disables the command; without the no, enables or re-enables.
- Command or action. In some cases, *action* takes you to another command mode.
- Keyword or command within a submenu.
- Choose between the enclosed elements
- One or more repeated values



Many commands have a default setting or value, listed in the Default section of the command page.

Contacting Fortinet

You can visit Fortinet on the Internet at this URL:

<http://www.fortinet.com>

Click the Support menu button to view Fortinet Customer Services and Support information.

2 Key Concepts

This chapter presents tips for working with the command line interface (CLI). It describes the various command modes, provides some tips for getting help, using the history functions, and customizing the prompt and terminal characteristics. The following sections are included in this guide:

- [Getting Started on page 41](#)
- [CLI Command Modes on page 42](#)
- [Command Line-Only Commands on page 43](#)
- [Abbreviating Commands on page 45](#)
- [Using No and Default Forms of Commands on page 46](#)
- [Getting Help on page 47](#)
- [Using Command History on page 48](#)
- [Finding Words in show Command Output on page 49](#)
- [Customizing the CLI Prompt on page 50](#)
- [Manipulating Terminal Characteristics on page 50](#)
- [Ending a Session on page 51](#)
- [Password Spacing on page 51](#)

Getting Started

To start using the Command Line Interface:

1. Connect to the controller using the serial console or Ethernet port, or remotely with a telnet or SSH2 connection once the controller has been assigned an IP address.
To assign the controller an IP address, refer to the “Initial Setup” chapter of the **FortiAP and Radio Switch Installation Guide**
2. At the login prompt, enter a user ID and password. By default, the `admin` user IDs is configured and the `guest` user is disabled.
 - If you log in as the user `admin`, with the `admin` password, you are automatically placed in privileged EXEC mode.

- If you log in as the user `guest`, you are placed in user EXEC mode. From there, you must type the **enable** command and the password for user `admin` before you can enter privileged EXEC mode.
3. Start executing commands.

CLI Command Modes

The CLI is divided into different command modes, each with its own set of commands and in some modes, one or more submodes. Entering a question mark (?) at the system prompt provides a list of commands available at the current mode.

User EXEC Mode

When you start a session on the controller, you begin in user mode, also called user EXEC mode. Only a subset of the commands are available in user EXEC mode. For example, most of the user EXEC commands are one-time and display-only commands, such as the **show** commands, which list the current configuration information, and the **clear** commands, which clear counters or interfaces. The user EXEC commands are not saved when the controller reboots.

- Access method: Begin a session with the controller as the user `guest`.
- Prompt: `default>`
- Exit method: Enter **exit** or **quit**.
- Summary: Use this mode to change console settings, obtain system information such as showing system settings and verifying network connectivity.

Privileged EXEC Mode

To access all the commands in the CLI, you need to be in privileged EXEC mode. You can either log in as **admin**, or enter the **enable** command at the user EXEC mode and provide the **admin** password to enter privileged EXEC mode. From this mode, you can enter any privileged EXEC command or enter Global Configuration mode.

- Access method: Enter **enable** while in user EXEC mode, or log in as the user **admin**.
- Prompt: **default#**
- Exit method: Enter **disable**.
- Summary: Use this mode to manage system files and perform some troubleshooting. Change the default password (from Global Configuration mode) to protect access to this mode.

Global Configuration Mode

You make changes to the running configuration by using the Global Configuration mode and its many submodes. Once you save the configuration, the settings are stored and restarted when the controller reboots.

From the Global Configuration mode, you can navigate to various submodes (or branches), to perform more specific configuration functions. Some configuration submodes are **security**, **qosrules**, **vlan**, and so forth.

- Description: configures parameters that apply to the controller as a whole.
- Access method: Enter **configure terminal** while in privileged EXEC mode.
- Prompt: `controller(config)#`
- Exit method: enter **exit** or press **Ctrl-Z** to return to privileged EXEC mode (one level back).
- Summary: Use this mode to configure some system settings and to enter additional configuration submodes (**security**, **qosrules**, **vlan**).

Command Line-Only Commands

Many CLI commands have an equivalent functionality in the Web Interface, so you can accomplish a task using either interface. The following lists commands that have no Web Interface functionality.

EXEC Mode Commands

- `configure terminal`
- `no history`
- `no prompt`
- `no terminal length |width`
- `help`
- `cd`
- `copy` (including `copy running-config startup-config`, `copy startup-config running-config` and all local/remote copy)
- `delete flash: image`
- `delete filename`
- `dir [dirname]`
- `debug`
- `disable`
- `enable`

- exit
- quit
- more (including more running-config, more log *log-file*, more running-script)
- prompt
- rename
- terminal history|size|length|width
- traceroute
- show history
- show running-config
- show terminal

Config Mode Commands

- do
- ip ftp|scp|sftp *username*
- ip ftp|scp|sftp *password*
- show context

Commands that Invoke Applications or Scripts

- calendar set
- timezone set|menu
- date
- capture-packets
- analyze-capture
- debug
- diagnostics[-controller]
- ping
- pwd
- shutdown controller force
- reload controller default
- run
- setup
- upgrade
- downgrade
- packet-capture-profile
- poweroff

- show calendar
- show timezones
- show file systems
- show memory
- show controller cpu-utilization
- show processes
- show flash
- show high-availability
- show qosflows
- show scripts
- show station details
- show syslog-host
- show log
- autochannel
- high-availability
- telnet
- syslog-host

Abbreviating Commands

You only have to enter enough characters for the CLI to recognize the command as unique. This example shows how to enter the **show security** command, with the command show abbreviated to **sh**:

```
controller# sh security-profile default
```

```
Security Profile Table
```

Security Profile Name	: default
L2 Modes Allowed	: clear
Data Encrypt	: none
Primary RADIUS Profile Name	:
Secondary RADIUS Profile Name	:
WEP Key (Alphanumeric/Hexadecimal)	: *****
Static WEP Key Index	: 1
Re-Key Period (seconds)	: 0
Captive Portal	: disabled
802.1X Network Initiation	: off
Shared Key Authentication	: off

```

Pre-shared Key (Alphanumeric/Hexadecimal)      : *****
Group Key Interval (Seconds)                    : 0
PMK Caching                                     : disabled
Key Rotation                                    : disabled
Reauthentication                               : off
MAC Filtering                                   : off
Firewall Capability                             : none
Firewall Filter ID                             :
Security Logging                               : off

```

Security Profile Table

```

Security Profile Name                          : default
L2 Modes Allowed                              : clear
Data Encrypt                                   : none
Primary RADIUS Profile Name                   :
Secondary RADIUS Profile Name                 :
WEP Key (Alphanumeric/Hexadecimal)           : *****
Static WEP Key Index                          : 0
Re-Key Period (seconds)                       : 0
Enable Multicast Re-Key                       : off
Enable Captive Portal                         : disabled
802.1X Network Initiation                     : off
Enable Shared Key Authentication              : off
Pre-shared Key (Alphanumeric/Hexadecimal)     : *****
Enable Reauthentication                       : off
MAC Filtering                                 : on

```

Using No and Default Forms of Commands

Almost every configuration command has a **no** form. In general, use the **no** form to:

- Disable a feature or function.
- Reset a command to its default values.
- Reverse the action of a command.
- Use the command without the **no** form to reenable a disabled feature or to reverse the action of a **no** command.

Configuration commands can also have a **default** form. The **default** form of a command returns the command setting to its default. Most commands are disabled by default, so the **default** form is the same as the **no** form. However, some commands are enabled by default and have variables set to certain default values. In these cases, the **default** command

enables the command and sets variables to their default values. The reference page for the command describes these conditions; these are some examples:

```
corpwifi# default history
corpwifi# default terminal length
corpwifi# default terminal width
```

Getting Help

Entering a question mark (?) at the system prompt displays a list of commands for each command mode. When using context-sensitive help, the space (or lack of a space) before the question mark (?) is significant. To obtain a list of commands that begin with a particular character sequence, enter those characters followed immediately by the question mark (?). Do not include a space. This form of help is called word help, because it completes a word for you.

To list keywords or arguments, enter a question mark (?) in place of a keyword or argument. Include a space before the ?. This form of help is called command syntax help, because it reminds you which keywords or arguments are applicable based on the command, keywords, and arguments you already have entered.

TABLE 1: Examples of Help Commands

Command	Purpose
(prompt)# help	Displays a brief description of the help system.
(prompt) # <i>abbreviated-command?</i>	Lists commands in the current mode that begin with a particular character string.
(prompt)# <i>abbreviated-command</i> <Tab>	Completes a partial command name
(prompt)# ?	Lists all commands available in command mode
(prompt)# <i>command?</i>	Lists the available syntax options (arguments and keywords) for the command.
(prompt)# <i>command keyword ?</i>	Lists the next available syntax for this command.

The prompt displayed depends on the configuration mode.

You can abbreviate commands and keywords to the number of characters that allow a unique abbreviation. For example, you can abbreviate the **configure terminal** command to **config t**.

Entering the **help** command will provide a description of the help system. This is available in any command mode.

Using Command History

The CLI provides a history of commands that you have entered during the session. This is useful in recalling long and complex commands, and for retyping commands with slightly different parameters. To use the command history feature, you can perform the following tasks:

- Set the command history buffer size
- Recall commands
- Disable the command history feature

Setting the Command History Buffer Size

By default, the CLI records ten command lines in its history buffer. To set the number of command lines that the system will record during the current terminal session, and enable the command history feature, use the **terminal history** command:

```
controller# terminal history [size n]
```

The **terminal no history size** command resets the number of lines saved in the history buffer to the default of ten lines or number specified by size.

To display the contents of the history buffer, type **default history**:

```
controller# default history
```

To display the contents of the history buffer, type **terminal history**

```
controller# terminal history

 7 interface Dot11Radio 1
 8 end
 9 interface Fast Ethernet controller 1 2
10 show interface Dot11Radio 1
11 end
12 show interfaces FastEthernet controller 1 2
13 sh alarm
14 sh sec
15 sh security
```

Recalling Commands

To recall commands from the history buffer, use one of the following commands or key combinations:

- **Ctrl-P** or **Up Arrow** key. This recalls commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.
- **Ctrl-N** or **Down Arrow** key. Returns to more recent commands in the history buffer after recalling commands with Ctrl-P or the Up Arrow key.
- *!number*. Execute the command at the history list *number*. Use the **terminal history** or **show history** commands to list the history buffer, then use this command to re-execute the command listed by its sequence number.
- To list the contents of the history buffer, use the **show history** command:

```
controller# show history
```

Disabling the Command History Feature

The terminal history feature is automatically enabled. To disable it during the current terminal session, type **no terminal history** in either privileged or non-privileged EXEC mode:

```
controller# no terminal history
```

Finding Words in show Command Output

To quickly locate a word in the output of any **show** command, use the following command:

```
show argument | grep "string"
```

For this feature to work, only one **show** command can be the input to the **grep** and the **show** command cannot have arguments (for example, the form of the command such as **show ap 54**). The "*string*" is a literal, case-sensitive word to search for (such as AP-54), and must be enclosed in double quotation marks. Only one string search can be performed per command line.

As an example, to search for and display the entry for AP-54 in the output of the **show ap** command, use the command:

```
controller# show ap | grep "AP-54"
```

```
AP ID AP Name      Serial Number      Op State Availability  Runtime
Connectivity AP Model AP Type
```

54	AP-54	00:0c:e6:00:3e:a8	Disabled	Offline	3.1.4-25
None		AP201	Local		

AP Table(1 entry)

Customizing the CLI Prompt

Default CLI Prompt

By default, the CLI prompt consists of the system name followed by an angle bracket (>) for user EXEC mode or a pound sign (#) for privileged EXEC mode.

Commands to Customize CLI Prompt

To customize the CLI prompt for your system, use one of the following commands in Global Configuration mode:

TABLE 2: *Commands to Customize the CLI Prompt*

Command	Purpose
prompt <i>string</i>	Customizes the CLI prompt.
no prompt	Disables the display of the CLI prompt.
default prompt	Sets the prompt to the default, which is the hostname.

Manipulating Terminal Characteristics

Displaying Terminal Settings

To display the current terminal settings, including the screen length and width, type:

```
controller> show terminal

Terminal Length:      0
Terminal Width:       80
History Buffer Size:   10
```

Setting Terminal Screen Length and Width

By default, the terminal length is set to 0 rows, and the width is set to 80 columns. To override this default setting, and set the number of lines or character columns on the current terminal screen for the current session, use the following commands in user EXEC mode:

```
controller> terminal length screen-length
controller> terminal width characters
```

To reset the terminal length and width to the default values, use the default command:

```
controller> default terminal length
controller> default terminal width
```

Setting the terminal length to a non-zero value turns on paging. When the output length exceeds the terminal length, the output is paused and a `---More---` is displayed:

1. If the space bar is pressed at the `---More---` prompt, another page of output is displayed.
2. If the ENTER key is pressed at the `---More---` prompt, a single line of output is displayed.
3. If any other character at the `---More---` prompt, this signifies the end of output and the command prompt is displayed.

Ending a Session

To end a session, use the following command in either User or privileged EXEC mode:

```
controller> exit
```

Password Spacing

Due to limitations in the CLI interface, it can be challenging for users to enter password phrases that utilize spaces; these passwords were more easily changed in the WebUI, where the space could be added clearly. However, passwords with spaces can be added via the CLI by simply putting the password phrase in quotes:

```
default(15)# password "sample password"
default(15)#
```

Note that the password will be entered without the quotes, so the actual configured password will be **sample password** in the example above.

3

User Interface Commands

The commands in this chapter perform configuration for the user interface, such as changing the prompt, and terminal history and display features. Additionally, commands for working with the interface such as getting help, and exiting and entering command levels are described.

- [*? on page 54*](#)
- [*disable on page 55*](#)
- [*do on page 56*](#)
- [*enable on page 57*](#)
- [*end on page 58*](#)
- [*exit on page 59*](#)
- [*help on page 60*](#)
- [*prompt on page 62*](#)
- [*quit on page 63*](#)
- [*show history on page 64*](#)
- [*show terminal on page 65*](#)
- [*terminal history on page 66*](#)
- [*terminal history size on page 67*](#)
- [*terminal length on page 68*](#)
- [*terminal width on page 69*](#)

?

Displays a list of applicable subcommands at the command level used.

Syntax

?

Command Mode

All

Default

Usage

Help is available at any level of the CLI by typing the ?. At each level, use ? to view a list of all commands. Use ? after each command to see a list of applicable subcommands and options.

Examples

controller> ?

debug	Turns on debugging.
default	Reset to default values.
enable	Enables privileged mode.
exit	Exit the CLI.
help	Displays help information.
no	Disables various parameters.
prompt	Customizes the CLI prompt.
quit	Exit the CLI.
show	Displays various system parameters.
terminal	Displays or sets terminal characteristics.

Related Commands

[help](#) on page 60

disable

Exits privileged EXEC mode to user EXEC mode.

Syntax

disable

Command Mode

User EXEC

Default

NA

Usage

When working in privileged EXEC mode, use the **disable** command to enter user EXEC mode. Note the prompt changes from the # in privileged EXEC mode to the > in user EXEC.

Examples

The following command exits privileged EXEC mode and enters user EXEC mode:

```
controller# disable
controller>
```

Related Commands

[enable](#) *on page 57*

do

Executes a CLI command from any command mode.

Syntax

do *<command>*

command CLI command to be executed.

Command Mode

All configuration modes.

Default

NA

Usage

Use the **do** command to run an EXEC-level command (such as **copy**, **default**, or **show**) from global configuration mode or any of the configuration submodes.

Examples

The following command saves the current configuration to the file `startup-config` without having to return to the privileged EXEC mode:

```
controller(config)# do copy running-config startup-config
```

The following command shows the IP settings for the controller:

```
controller(config)# do show ip
Interface Number IP Address      NetMask      Gateway Address Assign-
ment Type Interface Mode
1              172.26.0.53   255.255.240.0  172.26.0.1    DHCP
active

          IP Addresses(1 entry)
controller#
controller(config)#
```

enable

Enters privileged EXEC mode.

Syntax

enable

Command Mode

User EXEC

Default

NA

Usage

Use the **enable** command in user EXEC mode to enter privileged EXEC mode, which allows you to perform configuration tasks and enter configuration submodes. Note the prompt changes from the > in user EXEC mode to the # in privileged EXEC.

Examples

The following command, issued in user EXEC mode, enters privileged EXEC mode after you enter the administrative password.

```
controller> enable
Password:
controller#
```

Related Commands

[*disable*](#) on page 55

end

Exits configuration mode and enters privileged EXEC mode.

Syntax

end

Command Mode

Default

NA

Usage

Use the **end** command in most configuration modes to exit that configuration mode and re-enter privileged EXEC mode.

Examples

The following exits the security profile and global configuration mode, and takes you to privileged EXEC mode:

```
controller(config-security)# end
controller#
```

Related Commands

[*exit*](#) **on page 59**

exit

In any configuration mode, exits that mode and enters the next-highest mode, or in user EXEC mode, exits the CLI.

Syntax

exit

Command Mode

All

Default

Usage

The **exit** command behaves differently, depending on which command mode you are in. If you are in any configuration mode, use the **exit** command to exit the mode and enters the next-highest mode. If you are in user or privileged EXEC mode, use the **exit** command to quit the CLI.

Examples

The following command exits the security profile configuration mode and enters the next-highest mode, global configuration mode:

```
controller(config-security)# exit  
controller(config)#
```

Related Commands

[quit](#) on page 63

help

Displays help information that describes each command.

Syntax

```
help
help <command>
```

command	Displays help for the specified command.
----------------	--

Command Mode

All

Default

Lists the commands available from the current command level.

Usage

The **help** command displays a list of system commands for the current command mode. The **help** command behaves differently than the **?** command, displaying a larger list of commands and subcommands. Typing **help** before a command gives a description of that command.

Examples

```
controller(config)# help radius-profile
radius-profile:
Manage RADIUS servers.
```

The following example shows the commands available from the **radius-profile** command submode:

```
forti-wifi(config-radius)# help
default          Set RADIUS profile parameters to default value.
description      Specifies the RADIUS node.
do              Executes an IOSCLI command.
end              Save changes, and return to privileged EXEC mode.
exit             Save changes, and return to global configuration mode.
help            Displays help information.
ip-address       Configures the IP address.
key             Configures the secret key.
mac-delimiter    Configures the MAC Delimiter.
no              Disabling RADIUS profile parameters.
```


password-type Configures the RADIUS Password Type.

**Related
Commands**

[?](#) *on page 54*

prompt

Changes the CLI prompt.

Syntax

prompt <*prompt-name*>
no prompt

prompt-name The name of the new prompt.

Command Mode

Privileged EXEC

Default

The default prompt name is *default*.

Usage

Use this command to change the prompt name on the CLI. Use the **no prompt** command to disable the terminal prompt for the session.

Examples

The following command changes the prompt name from **default** to **controller**:

```
default# prompt controller  
controller#
```

quit

Exits the CLI.

Syntax

`quit`

Command Mode

User EXEC

Default

NA

Usage

Use the **quit** command to exit the CLI.

Examples

The following command exits the CLI:

```
default# quit
```

Related Commands

[*exit*](#) *on page 59*

show history

Displays a list of the commands last issued in this session.

Syntax

show history

Command Mode

User and privileged EXEC modes

Default

The default history size is 10.

Usage

Use the **show history** command to list the commands you have recently entered. The number of commands that the history buffer displays is determined by the **terminal history size** command.

Examples

The following command displays the last 10 commands entered during this session:

```
default> show history
 26 access-list permit import acl
 27 exit
 28 show access-list permit
 29 configure terminal
 30 access-list deny on
 31 exit
 32 show access-list deny
 33 disable
default>
```

Related Commands

[*terminal history size*](#) **on page 67**

show terminal

Displays terminal settings.

Syntax

`show terminal`

Command Mode

User and privileged EXEC modes

Default

NA

Usage

Displays the current settings for the terminal, including the length, width, and history buffer size.

Examples

The following command displays the terminal settings:

```
controller# show terminal
Terminal Length:      50
Terminal Width:       80
History Buffer Size:   10
controller#
```

Related Commands

- [terminal history on page 66](#)
- [terminal history size on page 67](#)

terminal history

Displays a history of commands entered.

Syntax

```
terminal history
no terminal history
```

Command Mode

User and privileged EXEC modes

Default

The default history buffer size is 10.

Usage

Shows the 10 most recent commands at this terminal. Use the **no** form to disable this feature for the current session.

Examples

The following shows the last 10 entries at this terminal:

```
controller# terminal history
 15 prompt default
 16 show terminal
 17 show terminal
 18 terminal history
 19 show terminal
 20 terminal
 21 show terminal
 22 show terminal
 22 terminal history
 23 show terminal
controller#
```

Related Commands

- [show terminal on page 65](#)
- [terminal history size on page 67](#)

terminal history size

Changes the number of lines recorded in the history buffer.

Syntax

terminal history size <*historysize*>
no terminal history

historysize Number of lines recorded in the history buffer. Valid value is from 0 to 1,000.

Command Mode

User EXEC

Default

The default history size is 10.

Usage

Changes the number of lines displayed at the terminal. Zero (0) reduces the number of history lines displayed to none. The command **no terminal history** disables the history function.

Examples

The following command changes the history buffer size to save the last 33 commands:

```
controller# terminal history size 33
controller#
controller# show terminal
Terminal Length:      10
Terminal Width:       80
History Buffer Size:   33
```

Related Commands

- [show terminal on page 65](#)
- [terminal history on page 66](#)

terminal length

Adjusts the number of lines that display on the terminal.

Syntax

terminal length <*length*>

length Number of lines displayed on the terminal. The valid range is 0 to 256.

Command Mode

User and privileged EXEC modes

Default

Zero (0) lines

Usage

Displays the number of rows on the terminal. Setting this parameter to 0 displays line by line. Numbers greater than 0 display in a block or group length.

Examples

```
controller# terminal length 100
controller#
```

Related Commands

[*terminal width*](#) **on page 69**

terminal width

Adjusts the number of columns that display on the terminal.

Syntax

terminal width <*width*>

width Number of columns displayed on the terminal. The valid range is 0 80.

Command Mode

User and privileged EXEC modes

Default

Zero (0) lines

Usage

Displays the number of columns on the terminal. Setting this parameter to 0 displays column by column.

Examples

```
controller# terminal width 60
controller#
```

Related Commands

[terminal length](#) on page 68

4 File Management Commands

The commands in this chapter are used to manage the system files, including the system image and backup configuration files. Included are the commands to save configurations, upgrade and downgrade the FortiWLC (SD) version, and show information to help understand and manage the configuration.

- [*cd on page 72*](#)
- [*copy on page 73*](#)
- [*copy running-config on page 75*](#)
- [*delete on page 77*](#)
- [*dir on page 79*](#)
- [*downgrade on page 81*](#)
- [*more on page 82*](#)
- [*pwd on page 84*](#)
- [*rename on page 85*](#)
- [*run on page 86*](#)
- [*show controller file systems on page 87*](#)
- [*show flash on page 89*](#)
- [*show running-config on page 90*](#)
- [*show startup-config on page 91*](#)
- [*show scripts on page 92*](#)
- [*upgrade ap on page 93*](#)
- [*upgrade controller on page 95*](#)
- [*upgrade system on page 97*](#)

cd

Sets the current working directory.

Syntax

cd

cd <*directory*>

directory

Directory name to set as current working directory.

Command Mode

Privileged EXEC

Default

The default working directory is `images`.

Usage

Typing **cd** by itself changes to the default working directory (`images`). Also use the **cd** command with a directory name to set the current working directory to one of the following directories:

`ATS/scripts`

The directory containing AP boot scripts.

`capture`

The directory containing packet capture files.

`images`

The directory containing upgrade images.

Examples

The following commands change to the directory `ATS/scripts`, verifies the change, and then goes back to the default `images` directory:

```
controller# cd ATS/scripts
```

```
controller# pwd
```

```
ATS/scripts
```

```
controller# cd
```

```
controller# pwd
```

```
images
```

Related Commands

- [dir](#) on page 79
- [pwd](#) on page 84

copy

Copies files locally and remotely.

Syntax

```
copy filename ftp://<username>:<password>@server/filename (copy file to
remote location)
copy ftp://<username>:<password>@server/filename . (copy remote file to
local location)
copy filename scp://<username>:<password>@server/directory/filename (copy
file to remote location)
copy sftp://<username>:<password>@server/filename . (copy remote file to
local location)
copy filename tftp://server/filename (copy file to remote location)
copy tftp://server/filename . (copy remote file to local location)
```

filename	Name of the remote or local file.
ftp://<username>:<pass- word>@server	Use FTP to transfer the file between the controller and server, using a valid username on that server. The password can be included or a prompt for the password will be provided.
scp://username@server	Use SCP to transfer the file between the controller and server, using a valid username on that server.
sftp://<username>:<pass- word>@server	Use SFTP to transfer the file between the controller and server, using a valid username on that server. The password can be included or a prompt for the password will be provided.
tftp://server/	Use TFTP to transfer the file between the controller and server (no username needed).

Command Mode

Privileged EXEC

Default

NA

Usage

On a remote file system with an FTP or SSH server, copy files to or from the controller.

Examples

The first command copies the file `dflt_backup.dbu` to the remote location `user1@server1/home/backup/` using FTP. The second command copies the remote backup file back into the local directory (using the `.` (dot) which is a shortcut for the copied file name (`dflt_backup.dbu`)).

```
controller# copy dflt_backup.dbu ftp://user1@server1/home/backup/  
dflt_backup.dbu
```

```
FTP password:
```

```
controller#
```

```
controller# copy ftp://user1@server1/home/backup/dflt_backup.dbu .
```

```
FTP password:
```

```
controller#
```

copy running-config

Copies the running configuration to local flash or remote system.

Syntax

```
copy running-config startup-config
copy running-config ftp://username<:password>@server/directory/filename
copy running-config scp://username<:password>@server/directory/filename
copy running-config tftp://server/directory/filename
copy filename running-config
```

<code>ftp://username<:password>@server</code>	Use FTP to transfer the file between the controller and server, using a valid username on that server. The password can be included or a prompt for the password will be provided.
<code>scp://username@server</code>	Use SCP to transfer the file between the controller and server, using a valid username on that server.
<code>tftp://server/</code>	Use TFTP to transfer the file between the controller and server (no username needed).
<code>startup-config</code>	Start up configuration.
<code>filename</code>	File name of the file to use as the output of or input to the running-config.

Command Mode

Privileged EXEC

Default

The default is the current running configuration.

Usage

Use the **copy running-config** command to copy the current running configuration to the local flash configuration file that is started upon system bootup, **startup-config**, or to a remote server for use as a backup. When the remote server is used for the copy, the file can be transferred using FTP, SFTP, SCP, or TFTP. The destination filename is user-selectable.

This command also accepts a file name as input to the running-config, which changes the running configuration to the commands in the input file.

To retrieve the file from the remote location, use the **copy** command.

Examples

The following command copies the current running configuration to the location `user1@server1/home/backup/` using either FTP.

```
controller# copy running-config ftp://user1:mypwd@server1/home/backup/run-  
ning-config
```

Related Commands

copy on page 73

delete

Deletes a file or upgrade image from the system.

Syntax

```
delete <filename>  
delete flash: <filename>
```

filename	Name of file to delete.
flash: filename	Name of upgrade image to delete.

Command Mode

Privileged EXEC

Default

NA

Usage

Use this command to remove a file or an upgrade image. This command is helpful to delete older, unneeded image files that have been downloaded into the images directory, and that take up unnecessary space on the flash card. Check the contents of the images directory with the **dir** command or the **show flash** command.

Examples

The following command sequence lists the contents of `capture` directory, deletes the file `my_capture_file`, and relists the contents of the directory.

```
controller# cd capture  
controller# pwd  
/capture  
  
controller# dir  
dir  
total 1  
-rw-r--r--    1 root    root        28658 May 14 12:02 my_cap-  
ture_file  
controller# delete my_capture_file  
controller# dir  
total 0
```

The following command deletes the file 3.0-139 from flash memory:

```
controller# delete flash: 3.0-139
controller#
```

Related Commands

- [*dir*](#) on page 79
- [*pwd*](#) on page 84
- [*show flash*](#) on page 89

dir

Displays directory contents.

Syntax

```
dir
dir <directory>
```

directory Name of the directory to display.

Command Mode

Privileged EXEC

Default

Lists the current working directory.

Usage

Use **dir** to display a long listing of the contents of the current directory. Use the optional *directory* argument to specify another directory. Optional directories include:

```
ATS/scriptsThe directory containing the AP boot scripts.
backupThe directory containing the backup databases.
captureThe directory containing packet capture files.
imagesThe directory containing the system images.
scriptsThe directory containing the controller scripts.
```

Examples

The following commands list the name of the current directory and display its contents.

```
controller# dir
total 70
drwxr-xr-x   8 root    root      1024 Jan 30 19:00 forti-3.5-45
drwxrwxr-x   8 522     522        1024 Feb 21 19:34 forti-3.5-46
-rw-r--r--   1 root    root      3195 Feb 19 10:17 forti.user-diagnostics.Dickens.2008-02-19.02-17-17.tar.gz
-rw-r--r--   1 root    root      3064 Feb 21 08:50 forti.user-diagnostics.Dickens.2008-02-21.00-50-50.tar.gz
-rw-r--r--   1 root    root      2635 Feb 21 10:12 forti.user-diagnostics.Dickens.2008-02-21.10-12-54.tar.gz
-rw-r--r--   1 root    root      3336 Mar  5 05:54 forti.user-diagnostics.Dickens.2008-03-05.05-54-51.tar.gz
-rw-r--r--   1 root    root      2398 Feb 22 10:24 forti.user-diagnostics.default.2008-02-22.10-24-42.tar.gz
```

```

lrwxrwxrwx    1 root    root
forti-3.5-46/mibs/mibs.tar.gz
-rw-r--r--    1 root    root
-rw-r--r--    1 root    root
-rw-r--r--    1 root    root
-rw-----    1 root    root
controller# dir scripts
total 2
-rw-r--r--    1 root    root
controller#
28 Feb 21 08:50 mibs.tar.gz ->
16778 Feb 21 08:50 pre-upgrade-config
18588 Mar  6 02:56 script.log
11172 Mar  5 05:59 startup-config
1915 Feb 21 08:50 upgrade.log
1239 Feb 21 19:16 create_rules.cli

```

Related Commands

[pwd](#) on page 84

downgrade

Downgrades the system

Syntax

`downgrade system version`

Command Mode

Privileged EXEC

Default

NA

Usage

Use the **downgrade system** command to revert to a system image that was previously installed on the system. This downgrade affects the controller and all APs.

Use the **show flash** command to view a list of system images that you can downgrade to.

Examples

The following command downgrades the system.

```
controller# downgrade system 3.2-116
```

Related Commands

- [show flash on page 89](#)
- [upgrade system on page 97](#)

more

Displays detailed file or system information

Syntax

```
more running-config
more startup-config
more running-script
more file <pathname>
more log
```

Command Mode

Privileged EXEC

Default

Usage

Use this command to page through the various details about the system configuration, as contained in the running-config, startup-config, and system log (syslogd.log) files. With the file keyword, specify the complete pathname of the file to be viewed. The **more running-config** command is a synonym for the **show running-config** command.

To abort this command, press Ctrl-C.

Examples

The following is a partial display of the running-config output.

```
default# more running-config
configure terminal
no ip dhcp-passthrough
audit period 60
auto-ap-upgrade enable
optimization none
hostname forti-wifi
ip dhcp-server 10.0.0.10
ip address 192.168.10.2 255.255.255.0
ip default-gateway 192.168.10.1
ip domainname 10.0.0.10
qosvars admission admitall
qosvars ttl 0
qosvars udpttl 0
```

```
qosvars tcpttl 0
qosvars enable
qosvars bwscaling 100
qosvars intercell-periodicity 30
qosvars drop-policy head
rogue-ap detection
rogue-ap acl 00:0c:e6:02:9e:6f
rogue-ap acl 00:0c:e6:03:5f:67
rogue-ap acl 00:0c:e6:04:5f:67
rogue-ap acl 00:0c:e6:05:b0:7a
rogue-ap acl 00:0c:e6:06:26:df
rogue-ap acl 00:0c:e6:07:17:d5
rogue-ap acl 00:0c:e6:08:e9:29
```

Related Commands

[show running-config](#) **on page 90**

pwd

Displays the current working directory.

Syntax

`pwd`

Command Mode

Privileged EXEC

Default

The current working directory.

Usage

Use this command to see the full pathname of the current working directory.

Examples

```
controller# pwd
images
controller#
```

Related Commands

[*dir*](#) on page 79

rename

Renames local files.

Syntax

`rename <source> <file_dst>`

source	Name of original filename to rename
file_dst	Destination, or new name for filename

Command Mode

Privileged EXEC

Default

None

Usage

Use this command to rename a file.

Examples

The following command renames the file `dflt_backup.mbu` to `default_backup.mbu`.

```
controller# rename dflt_backup.mbu default_backup.mbu
controller#
```

Related Commands

[*dir*](#) on page 79

run

Executes the named script.

Syntax

`run <script_file>`

`script_file` The full pathname of the script to execute.

Command Mode

Privileged EXEC

Default

None

Usage

Use this command to run tests or other diagnostic applications and display their results on the screen.

Examples

```
controller# cd ATS/scripts
controller# dir
total 4
-rw-rw-r-- 1 root root 3922 Jan 13 10:05 jan01-config
controller# run jan01-config
```

show controller file systems

Displays information about the controller file system.

Syntax `show controller file systems`

Command Mode Privileged EXEC

Default NA

Usage This command displays information about the system directories and file systems. It provides the following information:

TABLE 3: *Output of show controller file systems*

Parameter	Description
Filesystem	Displays the file system name. If the item is a directory, it displays none .
1K blocks	Shows the number of 1K byte blocks the file system or directory is configured to use.
Used	Show the number of 1K byte blocks the file system or directory currently uses.
Available	Show the number of 1K byte blocks the file system or directory has available to use (free space).
Use %	Show the percentage of available blocks the file system or directory currently uses.
Mounted on	Shows the mount point where the file system is mounted or lists the pathname of the directory.

Examples The following command lists information about the system file system:

controller# `show controller file systems`

Filesystem 1k-blocks Used Available Use% Mounted on

/dev/hda2	428972	230456	175630	57%	/
none	4880	40	4840	1%	/dev/shm
none	19528	6256	13272	33%	/opt/forti/var/run
none	9764	2944	6820	31%	/opt/forti/var/log
none	9764	896	8868	10%	/tmp
none	9764	0	9764	0%	/opt/forti/capture

controller#

Related Commands

show flash

Displays the system image filenames in flash memory.

Syntax

show flash

Command Mode

Privileged EXEC

Default

NA

Usage

Use this command to see the flash image filenames.

Examples

The following command shows the flash image filenames.

```
controller# show flash
```

```
5.0-87
```

```
5.1-47
```

```
controller#
```

show running-config

Displays the current controller configuration.

Syntax

`show running-config`

Command Mode

Privileged EXEC

Default

NA

Usage

Use this command to view current system configuration parameters.

Related Commands

[more](#) on page 82

show startup-config

Displays the startup controller configuration.

Syntax

`show startup-config`

Command Mode

Privileged EXEC

Default

NA

Usage

Use this command to view the start-up system configuration parameters implemented when the controller starts up.

Related Commands

- [copy running-config on page 75](#)
- [more on page 82](#)

show scripts

Displays valid AP scripts.

Syntax

show scripts

Command Mode

EXEC

Default

NA

Usage

Use this command to display the name of valid AP scripts, for example a boot script for booting an AP. The following example describes copying a script, then shows the script after the copy is complete.

Examples

The following example describes copying a script, then shows the script after the copy is complete.

```
controller# cd ATS/scripts
controller# copy scp://jsmith@server2/home/jsmith/default-ap .
SCP Password:
default-ap          100% |*****| 3          00:00
controller# show scripts
default-ap
controller#
```


upgrade ap

Upgrades access point system image.

Syntax

```
upgrade ap <version>
upgrade ap same <id>
upgrade ap same <range>
upgrade ap same all
```

version

Version of FortiWLC-SD system image to be used during upgrade.

same <*id* | *range* | **all**>

Upgrades the access point image to the same version of system software that the controller is running.

- *id*—Upgrades the access point with the specified ID to the same version of system software that the controller is running.
- *range*—Upgrades a range of APs, specified as a list using commas and dashes, without spaces or wildcards. AP IDs must be listed in ascending order.
- **all**—Upgrades all access point image to the same version of system software that the controller is running.

Command Mode

Privileged EXEC

Default

NA

Usage

Before upgrading an access point's system image, transfer a compressed version of the image to the controller's images directory. The image must be in the images directory before you can upgrade. Use the **dir** command to see the images in that directory.

Transfer the new image file by using the **copy** command. For example, to use FTP to transfer the file, enter the following:

```
controller# copy ftp://jane@10.1.1.1/forti-3.2.tar .
```

If you have not configured a default FTP password using the **ip ftp password** command, you are prompted for a password.

To verify that the file was transferred properly, enter the following:

```
controller# show flash
3.2
```

When using the range option, the following types of

Examples

The following command upgrades to version 3.3 the access points with the IDs 1, 7, and 10:

```
controller# upgrade ap 3.3 1,7,10
```

The following command upgrades to version 3.3 the access points with the IDs 4 to 7, 10, and 12 to 20:

```
controller# upgrade ap 3.3 4-7,10,12-20
```

The following command upgrades all access points to the same version of the system image as the controller is running:

```
controller# upgrade ap same
```

This will overwrite all existing system images. Are you sure [y|n]? y

You see status of the upgrade process. When the upgrade is successful, you see a message similar to the following:

```
Upgrading APs
  1 AP-1          |=====| Success
controller#
```

Related Commands

[upgrade system](#) on page 97

upgrade controller

Upgrades system image for the controller.

Syntax

```
upgrade controller <version>  
upgrade controller <version> force
```

<i>version</i>	Version of the system image to be used during upgrade.
<i>force</i>	Force the upgrade. Required to upgrade to a current running version, such as when you need to revert an applied patch.

Command Mode

Privileged EXEC

Default

NA

Usage

Before you can upgrade a controller's system image, you must transfer a compressed version of the image to the controller /images directory. Use the dir command to see the current controller directory.

Transfer the new image file by using the copy command. For example, to use FTP to transfer the file, enter the following:

```
controller# copy ftp://jane@10.1.1.1/forti-5.1.tar .
```

If you have not configured a default FTP password using the **ip ftp password** command, you are prompted for a password.

To verify that the file was transferred properly, enter the following:

```
controller# show flash  
5.1
```

Examples

The following command upgrades the controller system image to version 5.1:

```
controller# upgrade controller 5.1-xx  
This will overwrite all existing system images. Are you sure [y|n]? y  
Upgrading Controller  
Stopping FortiWLC-SD services ...
```

```
Upgrading the current configuration ...  
Upgrade complete.
```

```
Broadcast message from root (pts/0) (Fri Mar 10 14:51:59 2004):
```

```
Now rebooting system...  
The system is going down for reboot NOW!  
default#
```

Related Commands

- [upgrade ap](#) on page 93
- [upgrade system](#) on page 97

upgrade system

Upgrades the controller and all access points.

Syntax

`upgrade system <version>`

version Version of the system image to be used during upgrade.

Command Mode

Global configuration

Default

NA

Usage

Before you can upgrade a system image, you must transfer a compressed version of the image to the controller `/images` directory. Use the **dir** command to see the current controller directory.

Transfer the new image file by using the **copy** command. For example, to use FTP to transfer the file, enter the following:

```
controller# copy ftp://jane@10.1.1.1/forti-5.1.tar .
```

If you have not configured a default FTP password using the **ip ftp password** command, you are prompted for a password.

To verify that the file was transferred properly, enter the following:

```
controller# show flash
5.1
```

Examples

The following command upgrades the controller and all access points to use the system image version 5.1:

```
controller# upgrade system 5.1
```

This will overwrite all existing system images. Are you sure [y|n]? **y**

Upgrading APs

```
1 AP-1 | | Success
```

Upgrading Controller

```
Stopping FortiWLC-SD services ...  
Upgrading the current configuration ...  
Upgrade complete.
```

```
Broadcast message from root (pts/0) (Fri Mar 10 14:51:59 2004):
```

```
Now rebooting system...  
The system is going down for reboot NOW!  
controller#
```

Related Commands

- [upgrade ap](#) on page 93
- [upgrade controller](#) on page 95

patch upgrade

Upgrades the controller and all access points to a patch.

Syntax

patch upgrade <version>

version Version of the patch imagee to be used during upgrade.

Command Mode

Global configuration

Default

NA

Usage

Before you can upgrade, you must transfer a compressed version of the image to the controller /images directory. Use the **dir** command to see the current controller directory.

Transfer the new image file by using the **copy** command. For example, to use FTP to transfer the file, enter the following:

```
controller# copy ftp://jane@10.1.1.1/forti-5.1.tar .
```

If you have not configured a default FTP password using the **ip ftp password** command, you are prompted for a password.

To verify that the file was transferred properly, enter the following:

```
controller# show flash
5.1
```

Examples

The following command upgrades the controller and all access points to use the system image version 6.1-3-6:

```
controller# patch system 6.1-3-6
```

This will overwrite all existing system images. Are you sure [y|n]? **y**

Upgrading APs

```
1 AP-1 | | Success
```

Upgrading Controller

Stopping FortiWLC-SD services ...

```
Upgrading the current configuration ...  
Upgrade complete.
```

```
Broadcast message from root (pts/0) (Fri Mar 10 14:51:59 2004):
```

```
Now rebooting system...  
The system is going down for reboot NOW!  
controller#
```

Related Commands

- [upgrade ap](#) on page 93

upgrade controller on page 95

5

System Management Commands

The commands in this chapter are used to manage the system. Tasks such as running the setup script, setting the system clock and timezXone, and obtaining system and networking information are included.

- [*10gig-module*](#) on page 106
- [*aeroscout*](#) on page 107
- [*alarm*](#) on page 108
- [*amconfig*](#) on page 111
- [*audit period*](#) on page 112
- [*bonding*](#) on page 113
- [*calendar set*](#) on page 115
- [*clear statistics interfaces*](#) on page 117
- [*client-locator*](#) on page 118
- [*controller-index*](#) on page 120
- [*date*](#) on page 121
- [*erase-guest-user*](#) on page 122
- [*event*](#) on page 123
- [*fastpath*](#) on page 126
- [*fingerprint*](#) on page 127
- [*guest-user*](#) on page 128
- [*hostname*](#) on page 130
- [*ip udp-broadcast downstream*](#) on page 131
- [*ip udp-broadcast downstream-bridged*](#) on page 132
- [*ip udp-broadcast upstream*](#) on page 133
- [*ip udp-broadcast upstream-bridged*](#) on page 134
- [*license*](#) on page 135
- [*management wireless*](#) on page 137
- [*nms-profile*](#) on page 138

- [nms-server](#) on page 139
- [nms-vpn-server](#) on page 140
- [ntp](#) on page 141
- [passwd](#) on page 142
- [ping](#) on page 143
- [poweroff controller](#) on page 144
- [proactive-spectrum-manager](#) on page 145
- [proxy-arp-filtering](#) on page 148
- [reload](#) on page 149
- [reload-gui](#) on page 151
- [reload-management](#) on page 152
- [reload-security](#) on page 153
- [reload-snmp](#) on page 154
- [reload-vpn](#) on page 155
- [reload-wapi](#) on page 156
- [remove-license](#) on page 157
- [roaming-domain](#) on page 158
- [setup](#) on page 161
- [setup](#) on page 161
- [show alarm](#) on page 163
- [show bonding](#) on page 169
- [show calendar](#) on page 171
- [show client-locator](#) on page 172
- [show controller](#) on page 173
- [show controller cpu-utilization](#) on page 177
- [show controller file systems](#) on page 178
- [show controller memory](#) on page 180
- [show controller processes](#) on page 182
- [show event](#) on page 185
- [show fastpath](#) on page 187
- [show features](#) on page 189
- [show fingerprints](#) on page 190
- [show flash](#) on page 191
- [show guest-user](#) on page 192

- [show hostname](#) on page 194
- [show ip udp-broadcast downstream all-ports](#) on page 197
- [show ip udp-broadcast downstream-bridged all-ports](#) on page 198
- [show ip udp-broadcast upstream all-ports](#) on page 199
- [show ip udp-broadcast upstream-bridged all-ports](#) on page 200
- [show interfaces accel](#) on page 193
- [show license](#) on page 195
- [show license-file](#) on page 201
- [show log](#) on page 202
- [show nms-server](#) on page 203
- [show ntp-server](#) on page 204
- [show roaming-domain](#) on page 205
- [show syslog-file](#) on page 207
- [show syslog-host](#) on page 209
- [show syslog-table](#) on page 210
- [show sys-summary](#) on page 212
- [show sys-summary ess](#) on page 214
- [show sys-summary general](#) on page 216
- [show sys-summary resources](#) on page 218
- [show sys-summary stations](#) on page 219
- [show sys-summary throughput](#) on page 220
- [show system-id](#) on page 221
- [show timezones](#) on page 222
- [spectrum-band](#) on page 223
- [start-ntp](#) on page 224
- [statistics period](#) on page 225
- [Sysconfig backup](#) on page 226
- [Sysconfig restore](#) on page 227
- [syslog-host](#) on page 228
- [telnet](#) on page 229
- [timezone](#) on page 230
- [topo-update](#) on page 233
- [traceroute](#) on page 234
- [zeronet-packet](#) on page 235

10gig-module

Enables and disables 10 gig module state.

Syntax

10gig-module <*option*>

option Enable or Disable

Command Mode

Global configuration

Default

Usage

Example

```
controller# configure terminal
controller(confi)# 10gig-module enable
```

aeroscout

Enables and disables interoperability with tag tracking in Aeroscout suite of products.

Syntax

```
aeroscout enable  
aeroscout disable  
aeroscout ip-address  
aeroscout port
```

Command Mode

Global configuration

Default

This feature is disabled by default.

Usage

FortiWLC (SD) implements AeroScout's tag (but not laptop) protocol for interoperability between the Fortinet Networks infrastructure (controllers and access points) and AeroScout's platform. Use the **ip-address** and **port** parameters to specify the IP and port used by the Aeroscout machine.

Example

This example enables Aeroscout:

```
controller(config)# aeroscout ?  
disable          (10) Disabling AeroScout Feature.  
enable           (10) Enabling AeroScout Feature.  
ip-address       (10) The Aeroscout engine IP address.  
port             (10) The Aeroscout engine port.  
  
controller(config)# aeroscout enable
```

alarm

Configure the alarm-type

Syntax

alarm *<alarm-type>*

You have to enter one of the following alarm type within double quotes:

- AP CPU Usage High
- AP Down
- AP Memory Usage High
- AP Radio Card Failure
- AP Runtime Error
- AP Software Version Mismatch
- AP Wireless Interface Down
- AP Wireless Interface Station Capacity Full
- Admin Login Failure
- Alarm History Full
- Alarm History Reaches Threshold
- CAC limit reached
- Certificate Error
- Certificate Installed
- Controller CPU Usage High
- Controller IP Address Change
- Controller Memory Usage High
- DFS Channel Update
- DHCP Address Pool Exhausted
- Event Log Full
- Event Log Reaches Threshold
- Fan Module Failure
- High Channel Utilization
- Interference Detected
- Link Down
- Low Channel Quality
- MIC Counter Measure Activation

- Master Down
- Power Module Failure
- Radius Server Failed
- Radius Server Restored Primary
- Radius Server Switchover Failure Accounting
- Radius Server Switchover
- Rogue AP Detected
- Software License Expired
- Software License Violated
- System ID Changed
- User 802.1x Authentication Failure
- User TKIP Message Integrity Check Failure
- Watchdog Failure

Command Mode

Privileged EXEC

Default

NA

Usage

Use this command to configure the alarms using the alarm-type.

Examples

```
MC3200(15)# configure terminal
MC3200(15)(config)# alarm "AP CPU Usage High"
MC3200(15)(config-alarm-configuration)#?
end (10) Save changes, and return to privileged EXEC mode.
exit (10) Save changes, and return to global configuration mode
reload-configuration (10) Reload Default Configuration of this alarm.
severity (10) Configures Severity of this alarm.
snmp (10) Enable/Disable Snmp for this alarm.
state (10) Enable/Disable this alarm.
syslog (10) Enable/Disable Syslog for this alarm.
threshold (10) Configures Threshold value for this alarm.
MC3200(15)(config-alarm-configuration)# snmp enable
MC3200(15)(config-alarm-configuration)# exit
```

```
MC3200(15)(config)#
```

Related Commands

[show alarm](#) on page 163

amconfig

Selects the active MC5000 BLK1C2F2 interface to either copper or SFP ports.

Syntax

```
amconfig copper  
amconfig sfp
```

copper	Use the copper ports.
sfp	Use the SFP ports.

Command Mode

Global configuration

Default

NA

Usage

This command is only needed when you mix copper connectors with SFP connectors on an MC5000. If the connectors all match, you do not need this command.

Examples

The following command configures the ports for copper:

```
controller# configure terminal  
controller(config)# amconfig copper  
controller(config)#
```

audit period

Configures how often the controller collects information about access points.

Syntax

audit period <period>

period

Amount of time that elapses before the controller collects information about access points. The valid value range is 0, 5 through 65,535 seconds.

Command Mode

Global configuration

Default

The default audit period is 60 seconds.

Usage

Normally, you do not need to change the audit period. The audit period affects the data collected for the following commands:

- show ap-assigned
- show ap-siblings
- show ap-discovered
- show topoap

The audit period also controls how often rogue AP alarms are cleared.

Setting 0 for the period disables the audit collection.

Examples

The following command sets the audit period to 120 seconds:

```
controller(config)# audit period 120  
controller(config)#
```

bonding

Enable/disables Ethernet port aggregation on supported controller platforms.

Syntax

```
bonding none  
bonding single  
bonding dual
```

Command Mode

Global configuration

Default

bonding is single

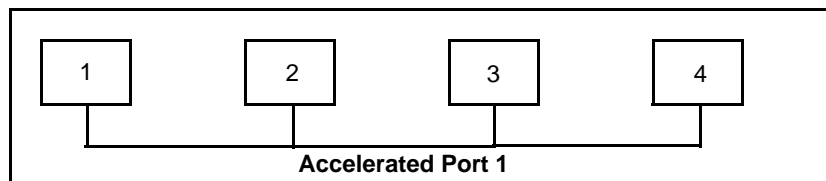
Usage

The **bonding** command allows applicable Ethernet ports to be used in parallel to increase throughput (also called port-trunking or link aggregation). This feature is supported on the MC4100 and MC5000 with AMC Ethernet port cards, as well as MC3200 and MC4200 controllers. When combined with FastPath mode acceleration, throughput is increased even further. Check the status of bonding with the **show controller** command.

Use the **bonding single** command to combine all four ports into one. The **bonding none** version removes bonding configuration and allows all ports to be used individually.

Controller reboot is required for the command to take effect unless the switch was setup for link aggregation before the controller was connected. Usually this is not the case and a reboot is required.

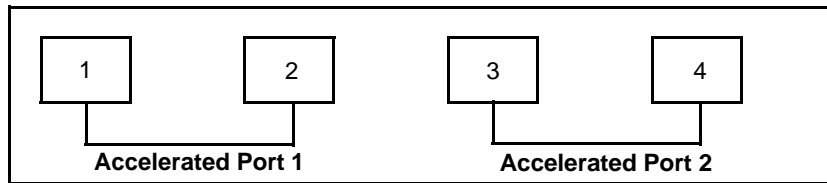
Figure 1: *Single Bonding*



Use the **bonding dual** command to combine the two sets of Ethernet ports into two accelerated ports.

Note that the Dual Ethernet mode requires the **bonding dual** setting.

Figure 2: *Dual Bonding*



Examples

The following command aggregates all MC4100 ports into one:

```
mc4100(config)# bonding single
```

Related Commands

- [fastpath](#) on page 126
- [show bonding](#) on page 169

calendar set

Sets the controller hardware and software clocks.

Syntax

calendar set <mm/dd/yyyy> <hh:mm:ss>

mm/dd/yyyy Date in month/day/year format (for example 04/06/2008).

hh:mm:ss Time in hours (24-hour format), minutes, and seconds.

Command Mode

Privileged EXEC

Default

NA

Usage

Use the **calendar set** command to manually set the system date and time. After setting the date and time, you are prompted to allow the controller to reboot. Answering **yes** at the prompt allows the system clock to be reset to the newly configured time. As well, you are prompted to save the running-config to the startup-config. Check the time settings with the **show calendar** or **date** commands.

Examples

The following command sets the system date and the hardware clock to the date of March 6, 2008 with a time of 1:00:00 p.m:

```
controller# calendar set 03/06/2008 13:00:00
```

```
This command requires a controller reboot. Do you want to Proceed [yes/no]
yes
```

```
Thu Mar 6 13:00:02 UTC 2008
```

```
You will lose any unsaved configuration. Save to startup-config now
[y|n]? y
```

```
Configuration saved
```

```
Broadcast message from root (Thu Mar 6 13:00:29 2008):
```

```
The system is going down for reboot NOW!
```

Related Commands

- [copy running-config](#) on page 75
- [show calendar](#) on page 171
- [date](#) on page 121

clear statistics interfaces

Resets statistics counter for the interface.

Syntax

```
clear statistics interfaces Dot11Radio <ap_id>
clear statistics interfaces FastEthernet controller
clear statistics interfaces FastEthernet ap <ap_id>
```

Command Mode

Privileged EXEC

Default

NA

Usage

Use the **clear statistics interfaces** commands to clear Dot11Radio or FastEthernet interface statistics. When clearing Dot11Radio statistics, an AP ID must be specified. When clearing FastEthernet statistics, you can specify the controller, all APs, or an AP by its ID.

Examples

This command clears all FastEthernet statistics on all APs:

```
controller# clear statistics interfaces FastEthernet ap
```

This command clears all FastEthernet statistics on AP 5:

```
controller# clear statistics interfaces FastEthernet ap 5
```

Related Commands

- [show interfaces Dot11Radio statistics on page 642](#)
- [show interfaces FastEthernet statistics on page 300](#)

client-locator

Controls the client location script.

Syntax

```
client-locator (Enables the client location script)  
no client-locator (Disables the client location script)  
show client-locator (Displays the state of the client Locator utility)  
client-locator add (adds OUIs to the locator)  
show client-locator ouis (displays OUIs present in the locator)
```

Command Mode

Privileged EXEC

Default

disabled

Usage

This feature sends ICMP packets to silent clients to make sure that the clients do not go to sleep. The silent client's OUI is entered in a predefined script named `ping_ouis locate` located in the folder `/opt/meru/bin`.

Users can also add specific OUIs and display the current list of them via the **add** and **show** commands.

Examples

```
controller# client-locator  
controller# sh client-locator  
Client Locator utility is enabled  
controller# no client-locator  
controller# sh client-locator  
Client Locator utility is disabled  
controller#  
  
controller# client-locator add 11:22:33  
controller#  
  
controller# show client-locator ouis  
00:13:02  
00:02:b3  
00:03:47
```

00:04:23
00:07:e9
00:0c:f1
00:0e:0c
00:0e:35
00:11:11
00:12:f0
00:13:20
controller#

Related Commands

none

controller-index

Sets controller identifier for per-station BSSID usage.

Syntax

controller-index <*identifier*>

identifier Unique identifier for the controller. *identifier* can be a value from 1-255. Setting *identifier* to 0 disables the option.

Command Mode

Global configuration mode

Default

Disabled (set to 0).

Usage

Use the **controller-index** command to uniquely identify a controller for use with the Virtual Port feature, where each station is assigned its own unique link which it keeps throughout the Virtual Cell. A unique controller index must be applied to each controller in the WLAN.

The controller index is part of the system information that is used to create a unique CSSID. Every client associated to an ESS that uses Virtual Port is assigned a CSSID. When the controller index changes, all clients assigned a CSSID must be disconnected and reconnected because the value of the CSSID also changes.



Do not apply the same index number to two different controllers on the same network.

Examples

This command sets the controller index to 1:

```
controller# configure terminal
controller(config)# controller-index 1
controller(config)# exit
```

Related Commands

[virtual-port](#) on page 567

date

Displays the current date and time.

Syntax

date

Command Mode

Privileged EXEC

Default

NA

Usage

Use the **date** command to display the current date and time. To set the system date and time, use the **calendar set** command.

Examples

This command displays the system date and time.

```
controller# date  
Thu Mar 6 13:15:34 UTC 2008
```

Related Commands

- [*calendar set on page 115*](#)
- [*show calendar on page 171*](#)

erase-guest-user

Erases the guest user table created by [guest-user on page 128](#) command.

Syntax

erase-guest-user

Command Mode

Privileged EXEC

Default

NA

Usage

Use the **erase-guest-user** command to erase the user table that was generated using the **guest-user** command.

Examples

This command erases the guest user table.

```
controller# erase-guest-user
```

Related Commands

[guest-user on page 128](#)

event

Configure the event-type

Syntax

event *<event-type>*

You have to enter one of the following event type within double quotes:

- AP CPU Usage High
- AP Down
- AP Memory Usage High
- AP Radio Card Failure
- AP Runtime Error
- AP Software Version Mismatch
- AP Wireless Interface Down
- AP Wireless Interface Station Capacity Full
- Admin Login Failure
- Alarm History Full
- Alarm History Reaches Threshold
- CAC limit reached
- Certificate Error
- Certificate Installed
- Controller CPU Usage High
- Controller IP Address Change
- Controller Memory Usage High
- DFS Channel Update
- DHCP Address Pool Exhausted
- Event Log Full
- Event Log Reaches Threshold
- Fan Module Failure
- High Channel Utilization
- Interference Detected
- Link Down
- Low Channel Quality
- MIC Counter Measure Activation

- Master Down
- Power Module Failure
- Radius Server Failed
- Radius Server Restored Primary
- Radius Server Switchover Failure Accounting
- Radius Server Switchover
- Rogue AP Detected
- Software License Expired
- Software License Violated
- System ID Changed
- User 802.1x Authentication Failure
- User TKIP Message Integrity Check Failure
- Watchdog Failure

Command Mode

Privileged EXEC

Default

NA

Usage

Use this command to configure the events using the event type.

Examples

```
MC3200(15)# configure terminal
MC3200(15)(config)# event "AP CPU Usage High"
MC3200(15)(config-event-configuration)#?
end (10) Save changes, and return to privileged EXEC mode.
exit (10) Save changes, and return to global configuration mode
reload-configuration (10) Reload Default Configuration of this alarm.
severity (10) Configures Severity of this alarm.
snmp (10) Enable/Disable Snmp for this alarm.
state (10) Enable/Disable this alarm.
syslog (10) Enable/Disable Syslog for this alarm.
threshold (10) Configures Threshold value for this alarm.
MC3200(15)(config-event-configuration)# snmp enable
MC3200(15)(config-event-configuration)# exit
```



```
MC3200(15)(config)#
```

Related Commands

[show event](#) *on page 185*

fastpath

Enables and disables Ethernet port acceleration.

Syntax

```
fastpath on  
fastpath off
```

Command Mode

Global configuration

Default

fastpath is enabled

Limitations

Only unicast IPv4 and UDP flows can be processed by **fastpath**

Usage

The **fastpath** utility accelerates the rate that packets are moved through the Ethernet interface, based on identification of an IP packet stream. When **fastpath** is enabled, the beginning of the IP packet stream is processed by the controller, and all subsequent packets of the same stream are forwarded according to the disposition of the initial packets, without being processed by the controller. This offloads a significant amount of processing from the controller.

Examples

The following disables fastpath acceleration:

```
controller(config)# fastpath off  
controller#
```

Related Commands

- [bonding](#) on page 113
- [capture-packets](#) on page 890

fingerprint

Device fingerprinting allows collection of various attributes about a device connecting to your network. The collected attributes can fully or partially identify individual devices, including the client's OS, device type, and browser being used. In previous versions of FortiWLC (SD), Station information included station's mac-address and its network activity. Device Fingerprinting can provide more information for the station and allows system administrators to be more aware of the types of devices in use and take necessary actions. You can view the details of the devices via **Monitor > Dashboard**. You can add, delete, or restore the devices using the fingerprint command and the command [show fingerprints on page 190](#) displays the device fingerprints stored in the system.

Syntax

fingerprint [add/delete] [*“description”*] [*“hexadecimal signature”*]

Command Mode

Global configuration

Default

n/a

Usage

Device fingerprints allow the system to detect and display stations' OS and type based on their hexadecimal signature. The **fingerprint** commands allow the user to add or remove fingerprints from the system.

Examples

```
controller(config)# fingerprint add “devicetype” “34e514d”
```

```
controller#
```

```
controller(config)# fingerprint delete “devicetype” “34e514d”
```

```
controller#
```

Related Commands

[show fingerprints on page 190](#)

guest-user

Creates a guest user account and enters guest-user submode.

Syntax

guest user <guestname>,<password>,<service start time>,<service end time>

guestname	name
password	password
service start time	Time that the user can start s using the account in the format “mm/dd/yyyy hh:mm:ss”
service end time	Time that the user can no longer access the account in the format “mm/dd/yyyy hh:mm:ss”

Command Mode

Global configuration

Default

None

Usage

The **guest-user** command allows a local administrator to add a guest account that provides a user temporary access from the Captive Portal. A maximum of 32 concurrent guest user accounts can exist. More than one guest user can use the same guest user account name.

The **guest-user** command creates a guest user account for the specified *name* and enters guest-user submode, where the remaining account details such as password, account activation start time and end time can be configured.

Once the account is created, when a user logs into the Captive Portal using the account name, the correct password must be supplied, and the login attempt must be made between the configured account start and end times for a successful login to occur.

Use the exact same command to edit an existing guest user.

Examples

This example configures a guest user.

```
MC3K-1(config)# guest-user ?
<guestname>          Enter the name of the guest user.
MC3K-1(config)# guest-user TempGuest ?
```

```

<password>          Enter the password of the guest user.
MC3K-1(config)# guest-user TempGuest XXXXX ?
<start-time>        Enter the service start-time (mm/dd/yyyy hh:mm:ss)
in double quotes.
MC3K-1(config)# guest-user TempGuest XXXXX "01/01/2010 00:00:00" ?
<end-time>          Enter service end-time (mm/dd/yyyy hh:mm:ss) in dou-
ble quotes.
MC3K-1(config)# guest-user TempGuest XXXXX "01/01/2010 00:00:00" "01/01/
2011 00:00:00" ?
<CR>
MC3K-1(config)# guest-user TempGuest XXXXX "01/01/2010 00:00:00" "01/01/
2011 00:00:00"
MC3K-1(config)# exit
MC3K-1# show guest-user

```

Guest User Name	Service
Start Time	Service End Time
TempGuest 00:00:00	01/01/2010 01/01/2011 00:00:00

Guest User Table(1 entry)

MC3K-1#

Related Commands

[show guest-user](#) on page 192

hostname

Specifies the hostname of the controller.

Syntax

hostname <*name*>

Command Mode

Global configuration

Default

None

Usage

Use this command to assign a hostname to the controller.

Examples

The following commands display the hostname (default), enters Global configuration mode, and assigns the label *mc1100* to the controller:

```
default# show hostname
default
default(config)# configure terminal
default(config)# hostname 3200
mc3200(config)# exit
mc3200# show hostname
mc3200
```

ip udp-broadcast downstream

Configures all UDP downstream ports for broadcast passthrough.

Syntax

```
ip udp-broadcast downstream all-ports on
ip udp-broadcast downstream all-ports selected
```

Command Mode

Configure terminal

Default

Selected ports are on by default.

Usage

You can use this command to configure all UDP downstream ports for passthrough by using the parameter **on**. The parameter **selected** means that up to eight ports named by the the legacy command **ip udp-broadcast downstream <portNumber>** are turned on. If you use the command **show ip udp-broadcast downstream all-ports** when the **selected** version of this command is active, you see a list of up to eight ports. We recommend that you use the **on** version of this command for testing purposes only.

```
default# configure terminal
default(config)# ip udp-broadcast downstream all-ports on
default(config)# end
default# show ip udp-broadcast downstream all-ports
Downstream UDP Broadcast All Ports

UDP All Ports : on
default#
```

Related Commands

- [ip udp-broadcast upstream on page 133](#)
- [ip udp-broadcast upstream-bridged on page 134](#)
- [show ip udp-broadcast downstream all-ports on page 197](#)
- [show ip udp-broadcast downstream-bridged all-ports on page 198](#)
- [show ip udp-broadcast upstream all-ports on page 199](#)
- [show ip udp-broadcast upstream-bridged all-ports on page 200](#)

ip udp-broadcast downstream-bridged

Configures all UDP downstream ports for broadcast bridged passthrough.

Syntax

```
ip udp-broadcast downstream-bridged all-ports on
ip udp-broadcast downstream-bridged all-ports selected
```

Command Mode

Configure terminal

Default

Selected ports are on by default.

Usage

You can use this command to configure all UDP downstream-bridged ports for passthrough by using the parameter **on**. The parameter **selected** means that up to eight ports named by the the legacy command **ip udp-broadcast downstream-bridged <portNumber>** are turned on. If you use the command **show ip udp-broadcast downstream-bridged all-ports** when the **selected** version of this command is active, you see a list of up to eight ports. We recommend that you use the **on** version of this command for testing purposes only.

```
default# configure terminal
default(config)# ip udp-broadcast downstream-bridged all-ports on
default(config)# end
default# show ip udp-broadcast downstream-bridged all-ports
Downstream UDP Broadcast All Ports
```

```
UDP All Ports : on
default#
```

Related Commands

- [*ip udp-broadcast downstream-bridged on page 132*](#)
- [*ip udp-broadcast upstream on page 133*](#)
- [*show ip udp-broadcast downstream all-ports on page 197*](#)
- [*show ip udp-broadcast downstream-bridged all-ports on page 198*](#)
- [*show ip udp-broadcast upstream all-ports on page 199*](#)
- [*show ip udp-broadcast upstream-bridged all-ports on page 200*](#)

ip udp-broadcast upstream

Configures all UDP upstream ports for broadcast passthrough.

Syntax

```
ip udp-broadcast upstream all-ports on
ip udp-broadcast upstream all-ports selected
```

Command Mode

Configure Terminal

Default

Selected

Usage

You can use this command to configure all UDP upstream ports for passthrough by using the parameter **on**. The parameter **selected** means that up to eight ports named by the legacy command **ip udp-broadcast upstream <portNumber>** are turned on. If you use the command **show ip udp-broadcast upstream all-ports** when the **selected** version of this command is active, you see a list of up to eight ports. We recommend that you use the **on** version of this command for testing purposes only.

Examples

```
default# configure terminal
default(config)# ip udp-broadcast upstream all-ports selected
default(config)# end
default# show ip udp-broadcast upstream all-ports
Upstream UDP Broadcast All Ports

UDP All Ports : selected
default#
```

Related Commands

- [ip udp-broadcast downstream on page 131](#)
- [ip udp-broadcast downstream-bridged on page 132](#)
- [show ip udp-broadcast downstream all-ports on page 197](#)
- [show ip udp-broadcast downstream-bridged all-ports on page 198](#)
- [show ip udp-broadcast upstream all-ports on page 199](#)
- [show ip udp-broadcast upstream-bridged all-ports on page 200](#)

ip udp-broadcast upstream-bridged

Configures all UDP upstream ports for broadcast bridged passthrough.

Syntax

```
ip udp-broadcast upstream-bridged all-ports on
ip udp-broadcast upstream-bridged all-ports selected
```

Command Mode

Configure Terminal

Default

Selected

Usage

You can use this command to configure all UDP upstream bridged ports for passthrough by using the parameter **on**. The parameter **selected** means that up to eight ports named by the legacy command **ip udp-broadcast upstream-bridged <portNumber>** are turned on. If you use the command **show ip udp-broadcast upstream-bridged all-ports** when the **selected** version of this command is active, you see a list of up to eight ports. We recommend that you use the **on** version of this command for testing purposes only.

Examples

```
default# configure terminal
default(config)# ip udp-broadcast upstream-bridged all-ports selected
default(config)# end
default# show ip udp-broadcast upstream-bridged all-ports
Upstream UDP Broadcast All Ports

UDP All Ports : selected
default#
```

Related Commands

- [ip udp-broadcast downstream on page 131](#)
- [ip udp-broadcast downstream-bridged on page 132](#)
- [show ip udp-broadcast downstream all-ports on page 197](#)
- [show ip udp-broadcast downstream-bridged all-ports on page 198](#)
- [show ip udp-broadcast upstream all-ports on page 199](#)
- [show ip udp-broadcast upstream-bridged all-ports on page 200](#)

license

Activates system licensing.

Syntax

```
license ftp://<host>/<filename>
```

host	Specifies the hostname where the license file resides. <i>host</i> can be a hostname or IP address.
filename	Specifies license file name.

Command Mode

Global configuration mode

Default

A license for 5 APs and a controller are configured as well as an Enterprise Mesh AP.

Usage

This command activates licenses for system hardware and feature modules. Licensing information is embedded within the controller firmware and is enabled with a Fortinet-generated license file. The license file is generated by Fortinet and contains the needed keys to license system components, based on the options the customer purchases.

Component licensing includes keys for the master or standby controller, and the maximum number of APs the master or standby controller associates (based upon controller model).

Feature licensing supports the following:

- Number of APs (maximum number of APs the controller uses based upon controller model)
- N+1 (ability to use one standby controller for multiple master controllers)
- Per-User Firewall (ability to define and apply firewall policies on a per-user basis)
- GRE tunneling (ability to tunnel selective traffic using ESS profile configuration)
- Dual B/G (ability to use both radios of AP208 on same frequency band)
- Enterprise Mesh

Upon receiving the licensing key file from Fortinet, place in the in the FTP directory (if using FTP) or SCP location of your choice.

Use the **no** form to remove the specified feature set from the system.

Examples

The following command obtains the license file `license17331.lic` from the FTP server at 192.168.1.10 and activates licensing for a controller:

```
mc3000(config)# license ftp://admin:admin@192.168.1.10/license17331.lic
```

Related Commands

- [*show license*](#) **on page 195**
- [*show license-file*](#) **on page 201**

management wireless

Enables or disables wireless management access to the controller.

Syntax

```
management wireless
no management wireless
```

Command Mode

Global Configuration mode

Default

Wireless management to the controller is enabled.

Usage

Use the **management wireless** command to allow wireless stations to enact configuration changes to the controller. If this presents a security problem for your site, you can disable the wireless access by using the **no management wireless** command; after which all packets except for VPN and Captive Portal that are sent by wireless clients are blocked.

Check the status of the management access with the **show controller** command. The line at the bottom of the output, `Management by wireless stations:` will show either an **on** or **off** value.

Examples

The following command disables controller configuration access to wireless stations:

```
controller# no management wireless
```

To re-enable access to wireless clients, use the command:

```
controller (config)# management wireless
```

Related Commands

[show controller](#) on page 173

nms-profile

Enable or Disable NMS profile.

Syntax

```
nms-profile enable  
nms-profile disable
```

Command Mode

Global configuration

Default

NA

Usage

Use this command to enable or disable the NMS profiling option.

Examples

The following command enables the NMS profile:

```
controller# configure terminal  
controller(config)# nms-profile enable  
controller(config)#
```

nms-server

Registers and unregisters the NMS Server.

Syntax

```
nms-server register  
nms-server unregister
```

Command Mode

Global configuration

Default

NA

Usage

Use this command to control use of the NMS Server. Network Management Systems (NMS) such as HP OpenView, and present alarm and trap information to configured management stations.

Examples

The following command registers the NMS Server:

```
controller# configure terminal  
controller(config)# nms-server register  
controller(config)#
```

nms-vpn-server

Configure an IP address for the NMS VPN server.

Syntax

nms-vpn-server <*ip address*>

Command Mode

Global configuration

Default

NA

Usage

Use this command to configure an IP address as NMS VPN server.

Examples

```
controller# configure terminal
controller(config)# nms-vpn-server 172.27.172.61
controller(config)#
```


ntp

Updates the system time by synchronizing the system clock with a specified Network Time Protocol (NTP) server.

Syntax

```
ntp sync
ntp server <server>
```

server IP address or hostname of the NTP server providing clock synchronization.

Command Mode

Privileged EXEC

Default

NA

Usage

Use the **ntp sync** command to enable periodic synchronization of the system clock with the NTP server specified with the **ntp server** command. Enabling NTP or changing the NTP server takes effect after a system reboot. Information about public NTP servers can be found at www.ntp.org.

To manually set the system clock, use the **calendar set** command.

Use the **date** command to check the system date and time.

Use the **show ntp-server** command to check the IP address of the assigned NTP server.

Examples

The following command performs NTP synchronization and specifies the NTP server with an IP address of 131.107.1.10:

```
controller# ntp sync
controller# ntp server 131.107.1.10
Setting NTP Server to 131.107.1.10. Change will only take effect after
reboot.
```

Related Commands

- [calendar set on page 115](#)
- [date on page 121](#)
- [show ntp-server on page 204](#)

passwd

Changes the admin or guest password.

Syntax

```
passwd admin  
passwd guest <password>
```

admin	Changes the administrative password.
guest	Changes the guest password.
password	The administrative or guest password.

Command Mode

Global configuration

Default

The default admin password is **admin**. The default guest password is **guest**.

Usage

After initially logging into the system, change the admin password. Follow standard Linux guidelines when changing passwords.

Examples

This example changes the default password for the admin:

```
MC5000-master# configure terminal  
MC5000-master(config)# passwd admin  
Changing password for user admin.  
New password:  
Retype new password:  
passwd: all authentication tokens updated successfully.  
MC5000-master(config)# end  
MC5000-master#
```

ping

Tests network connectivity.

Syntax

ping <hostname>

hostname IP address of the device to ping.

Command Mode

Privileged EXEC

Default

NA

Usage

Use the **ping** command to test basic network connectivity to a device.

Examples

The following command test the basic connectivity from the controller (10.3.1.2) to a device with an IP address of 10.3.4.5:

```
controller# ping 10.3.4.5
PING 10.3.4.5 (10.3.4.5) from 10.3.1.2 : 56(84) bytes of data.
64 bytes from 10.3.4.5: icmp_seq=1 ttl=255 time=0.334 ms
64 bytes from 10.3.4.5: icmp_seq=2 ttl=255 time=0.294 ms
64 bytes from 10.3.4.5: icmp_seq=3 ttl=255 time=0.276 ms
64 bytes from 10.3.4.5: icmp_seq=4 ttl=255 time=0.234 ms
64 bytes from 10.3.4.5: icmp_seq=5 ttl=255 time=0.311 ms

--- 10.3.4.5 ping statistics ---
5 packets transmitted, 5 received, 0% loss, time 3996ms
rtt min/avg/max/mdev = 0.234/0.289/0.334/0.040 ms
controller#
```

poweroff controller

Gracefully shuts down the controller.

Syntax

poweroff controller

Command Mode

Privileged EXEC

Default

NA

Usage

Use the **poweroff controller** command to gracefully shut down the controller.

Make sure you use the **copy running-config startup-config** command to save configuration changes to the startup configuration file before shutting down the controller if you want those changes to be available after you power on the controller.

Examples

The following command shuts down the controller:

```
controller# poweroff controller
```

```
Are you sure you want to poweroff the controller [y|n]? y
```

```
Broadcast message from root (pts/0) (Fri May 14 21:51:31 2004):
```

```
The system is going down for system halt NOW!
```

```
The controller is now shut down.
```

Related Commands

[copy running-config](#) on page 75

proactive-spectrum-manager

Monitors and suggests best channels of operation.

Syntax

```
proactive-spectrum-manager evaluate
proactive-spectrum-manager stop
proactive-spectrum-manager view
```

evaluate	Evaluates channel use and recommends or makes channel changes.
stop	Turns off PSM.
view	View mode monitors interference, such as rogues, and displays recommendations for channel use.

Command Mode

Privileged EXEC

Default

View is enabled on all channels by default.

Usage

You have two PSM options, View and Evaluate. View is enabled on all channels by default. View mode monitors interference, such as rogues, and displays GUI recommendations for channel use. If you see solid green bands on every channel in the charts, either only View is enabled or Evaluate is also enabled and there are no rogues on any channels.

Evaluate is disabled on all channels by default. If you enable Evaluate mode on the channels, then PSM will manage the use of those channels by moving devices away from channels with a specified amount of rogue activity.

Examples

The following command forces an immediate one-time evaluation of channel goodness: If the **Evaluation Time** was anything but zero, the evaluation would have continued to take place every x minutes, with x being the number you supplied for **Evaluation Time**. Only then (x is not zero) would you ever need to use the **stop** option to stop the repeating evaluation. Since this example selected **adapt**, channels will be changed if the difference between the existing channel and new channel is more than the value for **Adaptation Threshold** (default = 25%).

```
PSDMC1k# proactive-spectrum-manager
evaluate stop view
PSDMC1k# proactive-spectrum-manager evaluate
```

** Attention: Stations may be disconnected in this evaluation **

Are you absolutely sure [yes/No]? **yes**

Evaluation time [120s]?

View or Adapt [View/adapt]? **adapt**

Adaptation period [0] min (5-10080)? **5**

Adaptation threshold [25] %?

Interference detection for 120 s launched.

.....

Channel 1: goodness is N/A percent.

Channel 6: goodness is 100 percent.

Channel 11: goodness is N/A percent.

Channel 36: goodness is 0 percent.

Channel 40: goodness is N/A percent.

Channel 44: goodness is N/A percent.

Channel 48: goodness is N/A percent.

Channel 52: goodness is N/A percent.

Channel 56: goodness is N/A percent.

Channel 60: goodness is N/A percent.

Channel 64: goodness is N/A percent.

Channel 100: goodness is N/A percent.

Channel 104: goodness is N/A percent.

Channel 108: goodness is N/A percent.

Channel 112: goodness is N/A percent.

Channel 116: goodness is N/A percent.

Channel 120: goodness is N/A percent.

Channel 124: goodness is N/A percent.

Channel 128: goodness is N/A percent.

Channel 132: goodness is N/A percent.

Channel 136: goodness is N/A percent.

Channel 140: goodness is N/A percent.

Channel 149: goodness is N/A percent.

Channel 153: goodness is N/A percent.

Channel 157: goodness is N/A percent.

Channel 161: goodness is N/A percent.

Channel 165: goodness is N/A percent.

Channel pair 1,6: goodness is 100 percent.

Channel pair 6,11: goodness is 100 percent.

Channel pair 36,40: goodness is 0 percent.
 Channel pair 44,48: goodness is N/A percent.
 Channel pair 52,56: goodness is N/A percent.
 Channel pair 60,64: goodness is N/A percent.
 Channel pair 100,104: goodness is N/A percent.
 Channel pair 108,112: goodness is N/A percent.
 Channel pair 116,120: goodness is N/A percent.
 Channel pair 124,128: goodness is N/A percent.
 Channel pair 132,136: goodness is N/A percent.
 Channel pair 140,149: goodness is N/A percent.
 Channel pair 153,157: goodness is N/A percent.
 Channel pair 161,165: goodness is N/A percent.
 Recommended BG-channel of operation is 6.
 Recommended BG 40MHz channel of operation is 1,6.
 Recommended A-channel of operation is 36.
 Recommended A 40MHz channel of operation is 36,40.

*****check to see if channels changed*****

PSDMC1k# **show interfaces Dot11Radio**

AP ID	AP Name	IfIndex	AP Model	Admin	State	Op	State	Channel	Oper	Channel
Short	Preamble	RF	Band	AP	Mode					

1	AP-1	2	AP320	Up	Enabled	36	36	off	802.11a	Normal
---	------	---	-------	----	---------	----	----	-----	---------	--------

1	AP-1	1	AP320	Up	Enabled	6	6	on	802.11bgn	Normal
---	------	---	-------	----	---------	---	---	----	-----------	--------

The following command triggers Proactive Spectrum Manager to adapt (evaluate channels and make a one-time adjustment of channel use):

mg-mc2# **proactive-spectrum-manager evaluate**

** Attention: Stations may be disconnected in this evaluation **

Are you absolutely sure [yes/No]? **yes**

Evaluation time [120s]? **10**

View or Adapt [View/adapt]? **adapt**

Adaptation period [0] min (5-10080)? **0**

proxy-arp-filtering

Allows KDDI phones to be recognized by the controller after a soft handoff.

Syntax

```
proxy-arp-filtering enable
proxy-arp-filtering disable
```

Command Mode

Privileged EXEC

Default

Proxy-arp-filtering is disabled by default

Usage

This command affects the way a controller sends an ARP reply in response to an ARP request by a mobile station. If this flag is **enabled** (by default it is **disabled**), a controller does not respond to an ARP request whose target IP doesn't belong to the subnet of the mobile station's VLAN. This command allows a controller to recognize KDDI phones after handoff.

Examples

```
default#
default# proxy-arp-filtering enable
default#
default#
default# proxy-arp-filtering disable
default#
```

Related Commands

reload

Reboots the controller and access points.

Syntax

```
reload all
reload ap
reload ap <node-id>
reload controller
reload controller force
reload default
reload default factory
```

all	Reboots the controller and all access points.
ap [node-id]	Reboots all access points if no node ID is specified. Specify a node ID to reboot a specific access point.
controller [force]	Reboots only the controller. With the optional force option, forces a controller reboot with the last saved startup configuration. The force option should only be used in situations when there is no response from the controller.
default	<p>Reboots the controller and restores the passwords and system configuration to the original factory settings. Additionally, the AP script files (in /ATS/scripts/*) are deleted.</p> <p>WARNING: This option should be used rarely, if at all, as it may remove some files necessary for system operation.</p>



In an N+1 network, the reload command will not initiate failover.
This command cannot be executed in a active slave controller.

Command Mode

Privileged EXEC

Default

NA

Usage

In a high availability environment, use the **reload all** command when rebooting so that the master and backup controllers use the same configuration.

Examples

The following command reboots the access point with the node ID of 2:

```
controller# reload ap 2
```

Related Commands

- [*reload-gui*](#) **on page 151**
- [*reload-management*](#) **on page 152**
- [*reload-security*](#) **on page 153**
- [*reload-snmp*](#) **on page 154**
- [*reload-vpn*](#) **on page 155**
- [*reload-wapi*](#) **on page 156**

reload-gui

Resets the Web UI process.

Syntax

`reload-gui`

Command Mode

Privileged EXEC

Default

NA

Usage

The command **reload-gui** resets the Web UI process. Use this command if you experience Web UI issues such as:

- Web UI has become unreachable
- Data in the Web UI graphs are not updating
- AP Table page is frozen
- Web UI has become unstable

Examples

The following command reloads the Web UI.

```
controller# reload-gui
```

Related Commands

- [*reload*](#) on page 149
- [*reload-management*](#) on page 152
- [*reload-security*](#) on page 153
- [*reload-snmp*](#) on page 154
- [*reload-vpn*](#) on page 155
- [*reload-wapi*](#) on page 156

reload-management

Resets the controller management process.

Syntax

reload-management

Command Mode

Privileged EXEC

Default

NA

Usage

Use this command to reset the controller management process after the message “System Busy” puts the system in a non-responsive state. The command places the system back in a working mode.

Examples

The **reload-management** command resets the management process after the System Busy error message displays:

```
forti-wifi# show ap
The system is busy. Please try again.
forti-wifi#
forti-wifi# reload-management
```

Related Commands

- [reload](#) on page 149
- [reload-gui](#) on page 151
- [reload-security](#) on page 153
- [reload-snmp](#) on page 154
- [reload-vpn](#) on page 155
- [reload-wapi](#) on page 156

reload-security

Resets the security module.

Syntax

reload-security

Command Mode

Privileged EXEC

Default

NA

Usage

The command **reload-security** restarts all security-related processes on the system. Use it to reapply all security configurations currently saved.

Examples

The following command reloads the security module.

```
controller# reload-security
```

Related Commands

- [reload on page 149](#)
- [reload-gui on page 151](#)
- [reload-management on page 152](#)
- [reload-snmp on page 154](#)
- [reload-vpn on page 155](#)
- [reload-wapi on page 156](#)

reload-snmp

Resets the SNMP process.

Syntax

`reload-snmp`

Command Mode

Privileged EXEC

Default

NA

Usage

The command **reload-gui** resets the Web UI process. Use this command if you experience SNMP problems

Examples

The following command reloads the SNMP module.

```
controller# reload-snmp
```

Related Commands

- [reload on page 149](#)
- [reload-gui on page 151](#)
- [reload-management on page 152](#)
- [reload-security on page 153](#)
- [reload-vpn on page 155](#)
- [reload-wapi on page 156](#)

reload-vpn

Resets the VPN process.

Syntax

`reload-vpn`

Command Mode

Privileged EXEC

Default

NA

Usage

The command **reload-vpn** restarts the VPN configuration. Use this if users are having difficulty connecting via VPN APs.

Examples

controller# `reload-vpn`

Related Commands

- [reload](#) on page 149
- [reload-gui](#) on page 151
- [reload-management](#) on page 152
- [reload-security](#) on page 153
- [reload-snmp](#) on page 154
- [reload-wapi](#) on page 156
- [vpn server](#) on page 509

reload-wapi

Resets the WAPI process.

Syntax

reload-wapi

Command Mode

Privileged EXEC

Default

NA

Usage

The command **reload-wapi** resets the WAPI process. Use this command if you experience communication issues with the WAPI server.

Examples

The following command reloads the WAPI configuration.

```
controller# reload-wapi
```

Related Commands

- [reload](#) on page 149
- [reload-gui](#) on page 151
- [reload-management](#) on page 152
- [reload-security](#) on page 153
- [reload-snmp](#) on page 154
- [reload-vpn](#) on page 155
- [wapi-server](#) on page 356

remove-license

Removes licenses.

Syntax

`remove-license`

Command Mode

Privileged EXEC mode

Default

NA

Usage

This command removes licenses for system hardware and feature modules that have been added with the **license** command. Licensing information is embedded within the controller firmware and is enabled with a Fortinet-generated license file.

Invoking this command causes the controller to reboot.

Related Commands

[license](#) on page 135

roaming-domain

Configures a group of controllers that allow client roaming. This allows clients to roam between access points connected to two different controllers in the same subnet or different subnets

Syntax

```
roaming-domain create
roaming-domain start
roaming-domain stop
```

Command Mode

Global configuration

Default

No roaming domain exists

Usage

Use the command **roaming-domain create** on each controller to set up the group of controllers participating in the roaming-domain. Then start the service on each controller with the command **roaming-domain start**. To disable the service, use the command **roaming-domain stop**.

A maximum of 6 controllers can participate in a roaming domain. For more explanation, see the chapter “Inter-Controller Roaming” in the *FortiWLC-SD Configuration Guide*.

There are two RAC modes, static and dynamic. For limitations, see the Roaming Across Controllers ” section in the *FortiWLC-SD Configuration Guide*.

Examples

The following examples show how an RAC group is created on the first controller. This setup should be duplicated on all other controllers in the roaming domain.

Example of Dynamic Roaming Configuration

```
default(config)# roaming-domain create
Create Roaming Domain [y/n]?: y
-----
                Configure Roaming Domain
-----
```

When entering values, make sure they are identical in value and in identical order

among all participating controllers! Remember to include the current controller!

ESSID for this roaming domain, or q to quit:

IP address of a controller in roaming domain, or q to quit: **192.168.2.1**

Is 192.168.2.1 correct [y/n]?: **y**

IP address of a controller in roaming domain is 192.168.2.1

Is this controller Static DHCP home for this roaming domain [y/n]? **:n**

IP address of a controller in roaming domain, or q to quit: **192.168.2.2**

Is 192.168.2.2 correct [y/n]?: **y**

IP address of a controller in roaming domain is 192.168.2.2

Is this controller Static DHCP home for this roaming domain [y/n]? **:n**

IP address of a controller in roaming domain, or q to quit: **q**

Roaming Domain configured!

Example of Static Roaming

default(config)# **roaming-domain create**

Create Roaming Domain [y/n]?: **y**

Configure Roaming Domain

When entering values, make sure they are identical in value and in identical order

among all participating controllers! Remember to include the current controller!

ESSID for this roaming domain, or q to quit: **fixed_home**

Is homelink correct [y/n]?: **y**

ESSID for this roaming domain is homelink

IP address of a controller in roaming domain, or q to quit: **192.168.2.1**

Is 192.168.2.1 correct [y/n]?: **y**

IP address of a controller in roaming domain is 192.168.2.1

Is this controller Static DHCP home for this roaming domain [y/n]? **:y**

IP address of a controller in roaming domain, or q to quit: **192.168.2.2**

Is 192.168.2.2 correct [y/n]?: **y**

```
IP address of a controller in roaming domain is 192.168.2.2
IP address of a controller in roaming domain, or q to quit: q
```

```
-----
```

```
Roaming Domain configured!
```

```
-----
```

Related Commands

[show roaming-domain](#) *on page 205*

setup

Starts the basic system configuration setup script.

Syntax

setup

Command Mode

Privileged EXEC

Default

NA

Usage

Use the **setup** script to configure the basic parameters to get the system up and running. As the script runs, you are prompted for information that establishes the communication parameters for the controller.

If you specify that the controller IP address be assigned using DHCP, you need to provide the following information:

- Hostname for the controller (the hostname cannot consist entirely of integers)
- DHCP server IP address (used to assign controller IP address)
- NTP server used to synchronize controller clock (optional)

To assign a static IP address, you need to provide the following information:

- Hostname for the controller (cannot be in the form of an IP address)
- IP address of the controller
- Subnet mask for the controller
- IP address of the controller's default gateway
- IP addresses for the local DNS servers
- Name of the local domain
- NTP server used to synchronize controller clock (optional)

A complete description of the setup script is provided in the ***FortiWLC-SD Getting Started Guide***.

Examples

To run the initial configuration script that steps you through basic system configuration, use the **setup** command (partial display follows):

```
default# setup
```

```
Begin system configuration ...
```

```
Country code configuration for this machine.
```

```
The country code is currently set to US
```

```
Would you like to change it [yes/no/quit]?:
```

```
.
```

```
.
```

```
.
```

show alarm

Displays uncleared alarms known to the controller.

Syntax

show alarm

Command Mode

Privileged EXEC

Default

NA

Usage

Displays pending and uncleared alarms known to the controller, including those for connected access points, showing the date and time of each alarm, its severity, and the originating node.

If there are no pending uncleared alarms, the following displays:

Alarms Table(No entries)

Examples

The following command displays the current pending alarms:

```
controller# show alarm  
Alarms Table
```

Alarm Type	Severity	Timestamp	Content
AP Down	Critical	2005/05/14 21:57:17	Access Point AP-1 (1)
AP Down	Critical	2005/05/14 21:57:14	Access Point AP-25 (25)

The following table describes the fields of the **show alarm** output:

Information	Description
Alarm Type	<p>Alarm type. One of the following:</p> <p>AP Down: The controller has lost contact with the access point. Either the Ethernet cable is not connected to the access point, or the access point is down.</p> <p>Watchdog Failure: The watchdog process is hung. The system must be rebooted to clear this failure.</p> <p>Rogue AP Detected: An unauthorized AP (and AP not in the Allowed list) has been detected.</p> <p>Certificate expired: The certificate has either expired or has not been used yet.</p>
Severity	The severity of the alarm (always Critical).
Timestamp	<p>Date and time of the alarm in UTC (<i>year/month/day hh:mm:ss</i>), where:</p> <p><i>year</i>=year</p> <p><i>month</i>= month number (01 - 12)</p> <p><i>day</i>= day number</p> <p><i>hh</i> = hour (00 - 23)</p> <p><i>mm</i> = minutes</p> <p><i>ss</i> = seconds</p>
Content	<p>Details about the alarm. For rogue access point alarms, the content field lists the MAC address, BSSID, and channel that the station uses. For access points that are down, the content field lists the AP name and number.</p>

Related Commands

[alarm](#) on page 108

show ap-neighbor

Displays neighboring AP's.

Syntax

```
show ap-neighbor
show ap-neighbor <AP ID> <InterfaceList>
show ap-neighbor details
```

Command Mode

Privileged EXEC

Default

NA

Usage

To find out how dense coverage is in a certain area, check on an AP's neighbors with these commands. Nearby APs are listed whether they are on the same controller or on a different controller, along with this information about the neighboring APs:

- AP ID
- Controller Index
- AP MAC address
- RSSI

Examples

This example shows the details of neighboring APs:

Engg-wifi-Main# **sh ap-neighbor details**

AP ID Number	Interface Id	Serial Number	Channel	Neighbor AP ID	Serial
	ControllerIndex	Current	RSSI		
8	1	00:0c:e6:04:fc:b5	11	10	
	00:0c:e6:04:f0:b6	18	-54		
8	2	00:0c:e6:04:fc:b5	149	10	
	00:0c:e6:04:f0:b6	18	-54		
8	1	00:0c:e6:04:fc:b5	11	11	
	00:0c:e6:04:fc:b7	18	-66		
8	2	00:0c:e6:04:fc:b5	149	11	
	00:0c:e6:04:fc:b7	18	-70		

8	1	00:0c:e6:04:fc:b5	11	5
00:0c:e6:05:06:07		0	-76	
8	1	00:0c:e6:04:fc:b5	11	15
00:0c:e6:05:eb:7c		18	-76	
8	2	00:0c:e6:04:fc:b5	149	15
00:0c:e6:05:eb:7c		18	-86	
8	2	00:0c:e6:04:fc:b5	149	13
00:0c:e6:05:eb:7d		18	-63	
8	1	00:0c:e6:04:fc:b5	11	4
00:0c:e6:07:9e:9b		18	-72	
8	2	00:0c:e6:04:fc:b5	149	4
00:0c:e6:07:9e:9b		18	-86	
3	1	00:0c:e6:05:eb:11	11	0
00:00:00:00:00:00		0	-40	
3	2	00:0c:e6:05:eb:11	11	6
00:0c:e6:00:68:3f		0	-84	
3	1	00:0c:e6:05:eb:11	11	4
00:0c:e6:04:3c:8f		0	-70	
3	1	00:0c:e6:05:eb:11	11	22
00:0c:e6:04:99:79		0	-64	
3	2	00:0c:e6:05:eb:11	149	1
00:0c:e6:04:fc:c7		18	-62	
3	1	00:0c:e6:05:eb:11	11	1
00:0c:e6:04:fd:dd		0	-44	
3	1	00:0c:e6:05:eb:11	11	5
00:0c:e6:05:06:07		0	-73	

This example shows the neighboring APs:

Engg-wifi-Main# **sh ap-neighbor**

AP ID	Interface	Id	Channel	Local APs	Remote APs	RSSI L1	RSSI
L2		RSSI L3	RSSI L4				
8	1	11	4	2	0	1	
5		0					
8	2	149	4	0	0	1	
2		1					
3	1	11	4	6	1	2	
7		0					
3	2	11	5	1	0	1	
4		0					

2	1		11	4	5	1	2
6		0					
2	2		11	5	1	1	0
3		1					
5	1		11	5	7	2	3
6		1					
5	2		11	4	1	1	0
3		1					
1	1		11	7	6	1	8
4		0					
1	2		11	6	1	0	4
3		0					
4	1		11	6	5	2	4
5		0					
4	2		11	9	1	0	2
5		2					
13	1		11	5	3	1	3
4		0					
13	2		11	6	1	1	1
4		0					
10	1		11	4	5	1	2
5		1					
10	2		11	5	1	1	2
2		0					
11	1		11	5	7	0	4
7		0					
11	2		11	5	1	0	2
2		1					
15	1		11	7	6	1	5
7		0					
15	2		11	8	1	0	2
5		2					

AP Neighbors Consolidated List(20 entries)

These commands display the Neighboring AP seen by a particular AP in a particular Interface.

Engg-wifi-Main# **sh ap-neighbor 1 1**

AP ID	Interface	Id	Serial Number	Channel	Neighbor	AP ID	Serial
Number		ControllerIndex	Current	RSSI			
1	1		00:0c:e6:04:fc:c7	11	0		
00:00:00:00:00:00		0		-79			

1	1	00:0c:e6:04:fc:c7	11	4
00:0c:e6:04:3c:8f	0		-49	
1	1	00:0c:e6:04:fc:c7	11	11
00:0c:e6:04:fc:b7	18		-65	
1	1	00:0c:e6:04:fc:c7	11	1
00:0c:e6:04:fd:dd	0		-42	
1	1	00:0c:e6:04:fc:c7	11	5
00:0c:e6:05:06:07	0		-55	
1	1	00:0c:e6:04:fc:c7	11	8
00:0c:e6:05:ca:05	0		-56	
1	1	00:0c:e6:04:fc:c7	11	2
00:0c:e6:05:ea:e8	18		-63	
1	1	00:0c:e6:04:fc:c7	11	3
00:0c:e6:05:eb:11	18		-57	
1	1	00:0c:e6:04:fc:c7	11	15
00:0c:e6:05:eb:7c	18		-52	
1	1	00:0c:e6:04:fc:c7	11	4
00:0c:e6:07:9e:9b	18		-63	
1	1	00:0c:e6:04:fc:c7	11	5
00:0c:e6:07:9f:1d	18		-65	

AP Neighbors List(11 entries)

Engg-wifi-Main# sh ap-neighbor 1 2

AP ID	Interface Id	Serial Number	Channel	Neighbor AP ID	Serial
Number	ControllerIndex	Current	RSSI		
1	2	00:0c:e6:04:fc:c7	11	6	
00:0c:e6:00:68:3f	0		-64		
1	2	00:0c:e6:04:fc:c7	149	11	
00:0c:e6:04:fc:b7	18		-81		
1	2	00:0c:e6:04:fc:c7	149	2	
00:0c:e6:05:ea:e8	18		-72		
1	2	00:0c:e6:04:fc:c7	149	3	
00:0c:e6:05:eb:11	18		-61		
1	2	00:0c:e6:04:fc:c7	149	15	
00:0c:e6:05:eb:7c	18		-61		
1	2	00:0c:e6:04:fc:c7	149	4	
00:0c:e6:07:9e:9b	18		-63		
1	2	00:0c:e6:04:fc:c7	149	5	
00:0c:e6:07:9f:1d	18		-71		

AP Neighbors List(7 entries)

show bonding

Displays the Ethernet port bonding statistics.

Syntax

```
show bonding
show bonding full
```

Adding the option **full** displays detailed bonding configuration information.

Command Mode

Privileged EXEC

Default

NA

Usage

Bonding uses Ethernet ports in parallel to increase throughput (also called port-trunking or link aggregation). This feature is supported on the MC4100 and MC5000 with AMC Ethernet port cards. When combined with FastPath mode acceleration, throughput is increased even further.

Examples

The following command displays MC4100 and MC5000 with AMC acceleration card port bonding statistics:

```
default# show bonding
Current bonding configuration = single
Master bonding interface 0:
  Master interface 0 num slave interfaces = 1
  Slave interface 0-0:
    Slave interface 0-0 link status = up
* Use 'show bonding full' to display more details.
default#
```

This example shows dual bonding configuration:

```
default# show bonding
Current bonding configuration = dual
Master bonding interface 0:
  Master interface 0 num slave interfaces = 1
  Slave interface 0-0:
```

```
Slave interface 0-0 link status           = up
Master bonding interface 1:
  Master interface 1 num slave interfaces = 1
  Slave interface 1-0:
    Slave interface 1-0 link status       = down
* Use 'show bonding full' to display more details.
default#
```

Related Commands

[bonding](#) on page 113

show calendar

Displays the current date and time of the hardware clock.

Syntax

show calendar

Command Mode

Privileged EXEC

Default

NA

Examples

The following command displays the current date and time according to the hardware clock:

```
controller# show calendar
Thu Mar  6 14:00:12 UTC 2008
controller#
```

Related Commands

- [calendar set on page 115](#)
- [date on page 121](#)

show client-locator

Sends ping packets to specific OUI(s) connected to a Fortinet system.

Syntax

```
show client-locator
no client-locator
```

Command Mode

Privileged EXEC

Default

NA

Usage

This command is used to send ping packets to specific OUI(s) connected to a Fortinet system. This command is used mainly for clients that are silent.

Examples

This example enables client locator and disables it.

```
corpwifi# client-locator
corpwifi# sh client-locator
Client Locator utility is enabled
corpwifi# no client-locator
corpwifi# sh client-locator
Client Locator utility is disabled
```

Related Commands

show controller

Displays controller configuration information.

Syntax `show controller`

Command Mode Privileged EXEC

Default NA

Usage Use the `show controller` command to see global parameters for the controller. The display provides the following information about the controller:

Parameter	Description
Controller ID	The identification number of the controller.
Description	Optional text that identifies the controller.
Host Name	The hostname of the controller.
Uptime	The amount of time since the controller was booted.
Location	Optional text to help identify the location of the controller.
Contact	Option text to help identify the person or group to contact when this controller needs administration help.
Operational State	Operational state of the controller. If the controller is operating, the state is enabled , if not, the state is disabled .
Availability Status	Availability of this controller. The controller can be online or offline .
Alarm State	The alarm state can be No Alarms or the state of the alarm such as Critical .
Automatic AP Upgrade	On indicates that the controller will automatically upgrade the AP to the version of software running on the controller when the AP associates with the controller. Off indicates this feature is inactive.

Parameter	Description
Virtual IP Address	Virtual IP address assigned to the controller.
Virtual Netmask	Virtual netmask assigned to the controller.
Default Gateway	IP address of the default gateway.
DHCP Server	If dynamic addressing is assigned to this controller, displays the IP address of the server that DHCP requests are being forwarded to.
Statistics Polling Period (seconds)	The amount of time that must elapse before the controller polls for statistic information (for example, the number of packets passed or dropped).
Audit Polling Period (seconds)	The amount of time that must elapse before the controller collects audit information.
Software Version	The version of software running on the controller.
Network Device ID	The serial number (MAC address) of the controller.
System ID	The system identification of the controller.
Default AP Init Script	The name of the default initialization script that is run for access points that have no script specified. The scripts must reside in the directory <code>/ATS/scripts</code> .
DHCP Relay Pass-Through	Indicates whether pass-through mode is enabled for the DHCP Relay server.
Encryption Module Status	Displays whether the optional encryption processing module is present in the controller. If installed, this parameter displays Online . If not installed, this parameter displays Not Installed .
Controller Model	Lists the controller model.
Region Setting	Specifies whether the controller is an International or US-Only model (used for DFS purposes).
Country Setting	Displays the name of the country where the controller is located.
Manufacturing Serial #	Controller's serial number.
Management by wireless stations	If set to on , enables wireless management access to the controller; otherwise, if set to off , changes cannot be made wirelessly.

Parameter	Description
Controller Index	If Virtual Cell is set, shows 0 when Virtual Port is off or a number if Virtual Port is configured.
Topology Information Update	The Topology Information Update is useful for troubleshooting and collecting debug information. It is recommended that you enable this feature only if you need to collect troubleshooting and debug information.
AeroScout	If Aeroscout is enabled, tracking for tags is enabled. AeroScout has different messages for Tags than for Mobile Units such as laptops. Fortinet supports asset tracking of tags.
FastPath Mode	When FastPath mode is on , it accelerates throughput.
Bonding Mode	Bonding mode can be single or dual . Bonding uses Ethernet ports in parallel to increase throughput (also called port-trunking or link aggregation). This feature is supported on the MC4100 and MC5000 with AMC Ethernet port cards. When combined with Fast-Path mode acceleration, throughput is increased even further.
DFS	When DFS is enabled , replication to synchronize data is done on all servers that host a particular folder.
Station Aging Out Period (minutes)	

Examples

The following command displays controller configuration information:

```
InteropLab# show controller
Global Controller Parameters
```

```
Controller ID           : 1
Description             : InteropLab
Host Name               : InteropLab
Uptime                 : 47d:18h:55m:55s
Location               : DC Cabinet 6
Contact                : Network Group
Operational State       : Enabled
Availability Status     : Online
Alarm State            : No Alarm
```

```

Automatic AP Upgrade           : off
Virtual IP Address             : 172.26.96.11
Virtual Netmask                 : 255.255.255.0
Default Gateway                 : 172.26.96.1
DHCP Server                     : 10.0.0.10
Statistics Polling Period (seconds)/0 disable Polling : 60
Audit Polling Period (seconds)/0 disable Polling      : 60
Software Version                : 4.0-15
Network Device Id               : 00:90:0b:0e:a8:61
System Id                       : 1FC4B274070D
Default AP Init Script          :
DHCP Relay Passthrough          : on
Controller Model                 : MC1000
Country Setting                 : United States Of
America
Manufacturing Serial #          : 2008MC10001039
Management by wireless stations : on
Controller Index                 : 0
Topology Information Update      : off
AeroScout Enable/Disable        : disable
FastPath Mode                   : on
Bonding Mode                     : single
DFS                             : disable
Station Aging Out Period(minutes) : 0
InteropLab-MC1000#

```

Related Commands

- [*show controller cpu-utilization on page 177*](#)
- [*show controller file systems on page 178*](#)
- [*show controller memory on page 180*](#)
- [*show controller processes on page 182*](#)

show controller cpu-utilization

Show the controller CPU usage.

Syntax `show controller cpu-utilization`

Command Mode Privileged EXEC

Default NA

Usage Use the `show controller cpu-utilization` command to see CPU usage information for the controller. The display includes general usage information as well as a list of the top running processes that is updated in real time. Use a CTRL-C to return to the CLI prompt. CPU utilization is the CPU time used divided by the time the process has been running (cputime/realtime ratio), expressed as a percentage. It will probably not add up to 100%.

Examples The following command displays controller CPU utilization information:

```
controller# show controller cpu-utilization
```

Related Commands

- [show controller on page 173](#)
- [show controller file systems on page 178](#)
- [show controller memory on page 180](#)
- [show controller processes on page 182](#)

show controller file systems

Displays information about the file systems on the controller.

Syntax

`show controller file systems`

Command Mode

Privileged EXEC

Default

NA

Usage

This command displays information about the system directories and file systems. It provides the following information:

Parameter	Description
Filesystem	Displays the file system name. If the item is a directory, it displays none .
1K blocks	Shows the number of 1K byte blocks the file system or directory is configured to use.
Used	Show the number of 1K byte blocks the file system or directory currently uses.
Available	Show the number of 1K byte blocks the file system or directory has available to use (free space).
Use %	Show the percentage of available blocks the file system or directory currently uses.
Mounted on	Shows the mount point where the file system is mounted or lists the pathname of the directory.

Examples

The following command shows the controller file system information:

```
controller# show controller file systems
```

Filesystem	1k-blocks	Used	Available	Use%	Mounted on
/dev/hdc	420453	145615	252426	37%	/
none	4880	40	4840	1%	/dev/shm
none	9764	4820	4944	50%	/var/run
none	9764	308	9456	4%	/var/log
none	9764	0	9764	0%	/tmp
none	9764	0	9764	0%	/capture
controller#					

**Related
Commands**

- [show controller on page 173](#)
- [show controller cpu-utilization on page 177](#)
- [show controller memory on page 180](#)
- [show controller processes on page 182](#)

show controller memory

Displays memory used by running processes.

Syntax

```
show controller memory
show memory
```

Command Mode

Privileged EXEC

Default

NA

Usage

This command displays controller memory usage.

Examples

```
controller# show controller memory
total:      used:      free:  shared: buffers:  cached:
Mem:  527548416 237649920 289898496      0  6414336 129626112
Swap:           0           0           0
MemTotal:           515184 kB
MemFree:            283104 kB
MemShared:           0 kB
Buffers:             6264 kB
Cached:             126588 kB
SwapCached:          0 kB
Active:             140332 kB
Inact_dirty:         19204 kB
Inact_clean:         28012 kB
Inact_target:        37508 kB
HighTotal:           0 kB
HighFree:            0 kB
LowTotal:            515184 kB
LowFree:             283104 kB
SwapTotal:           0 kB
SwapFree:            0 kB
Committed_AS:       656468 kB
```


controller#

Related Commands

- [*show controller*](#) **on page 173**
- [*show controller cpu-utilization*](#) **on page 177**
- [*show controller file systems*](#) **on page 178**
- [*show controller processes*](#) **on page 182**

show controller processes

Displays information about all running controller processes.

Syntax `show controller processes`

Command Mode Privileged EXEC

Default NA

Usage This command displays a list of the controller processes. For each process, it lists the following information:

Parameter	Description
UID	(User ID) Displays the name of the user owning the process.
PID	(Process ID) Displays the ID number of the process.
PPID	(Parent Process ID) Shows the process number of the parent to this process.
C	
STIME	Shows the system time when the process was started.
TTY	Shows the terminal information where the process was started.
TIME	Shows the amount of time the process has been running.
CMD	Shows the name of the process.

Examples The following example shows a partial listing of the current system processes:

```
controller# show controller processes
UID      PID  PPID  C  STIME TTY      TIME  CMD
root      1    0  0 Oct14 ?        00:00:05 init
root      2    1  0 Oct14 ?        00:00:00 [keventd]
```

root	3	1	0	Oct14	?	00:00:04	[ksoftirqd_CPU0]
root	4	1	0	Oct14	?	00:00:00	[kswapd]
root	5	1	0	Oct14	?	00:00:00	[bdflush]
root	6	1	0	Oct14	?	00:00:00	[kupdated]
root	223	1	0	Oct14	?	00:00:00	syslogd -m 0
root	228	1	0	Oct14	?	00:00:00	klogd -x
root	238	1	0	Oct14	?	00:00:01	/usr/sbin/sshd

Related Commands

- [show controller](#) on page 173
- [show controller cpu-utilization](#) on page 177
- [show controller file systems](#) on page 178
- [show controller memory](#) on page 180

show controller mobility-vars

Displays information about adequate RSSI values.

Syntax `show controller mobility-vars`

Command Mode Privileged EXEC

Default NA

Usage This command displays current adequate RSSI value:

Parameter	Description
Topology Update	The Topology Information Update is useful for troubleshooting and collecting debug information. It is recommended that you enable this feature only if you need to collect troubleshooting and debug information. Select one of the following options: On: Enable the topology information update in the Controller. Off: Disable the topology information update. This is the default setting.
AssocStation-MaxIdle	Associated Station Max Idle Period value.
Adequate RSSI	The current configured adequate RSSI value.

Examples The following example shows the current RSSI value:

```
default (15)# show controller mobility-vars
Topology Update      AssocStationMaxIdle      Adequate RSSI
off                  2000                      -58
Controller Mobility Configuration Parameters(1 entry)
```

Related Commands

- [show controller on page 173](#)

show event

Displays uncleared events known to the controller.

Syntax

show event

Command Mode

Privileged EXEC

Default

NA

Usage

Displays pending and uncleared events known to the controller, including those for connected access points, showing the date and time of each event, its severity, and the originating node.

If there are no pending uncleared events, the following displays:

Events Table(No entries)

Examples

The following command displays the current pending events:

```
controller# show event
Events Table
```

Event Name	Severity	Source	FDN
Raised At	Detail	Information	

```
User 802.1x Authentication Fail Major      controller SD-ST-3-DAbcWebAuth-
00:23:1 07/26/2013 12:21:21 Acces
s Request rejected for User: <host/meru-it-THINK>, NAS IP: <172.29.0.137>,
SSID: <DAbcWebAuth>, Calling
Station ID: <00:23:14:ae:b9:28>, Called Station ID
```

```
User 802.1x Authentication Fail Major      controller SD-ST-3-DAbcWebAuth-
44:d8:8 07/26/2013 11:56:31 Acces
s Request rejected for User: <meru>, NAS IP: <172.29.0.137>, SSID: <DAb-
cWebAuth>, Calling Station ID: <
44:d8:84:b6:42:6d>, Called Station ID: <00:90:0b:23
```

The following table describes the fields of the **show event** output:

Information	Description
Event Type	Event type. One of the following: AP Down: The controller has lost contact with the access point. Either the Ethernet cable is not connected to the access point, or the access point is down. Watchdog Failure: The watchdog process is hung. The system must be rebooted to clear this failure. Rogue AP Detected: An unauthorized AP (and AP not in the Allowed list) has been detected. Certificate expired: The certificate has either expired or has not been used yet.
Severity	The severity of the event (always Critical).
Timestamp	Date and time of the event in UTC (<i>year/month/day hh:mm:ss</i>), where: <i>year</i> =year <i>month</i> = month number (01 - 12) <i>day</i> = day number <i>hh</i> = hour (00 - 23) <i>mm</i> = minutes <i>ss</i> = seconds
Content	Details about the event. For rogue access point alarms, the content field lists the MAC address, BSSID, and channel that the station uses. For access points that are down, the content field lists the AP name and number.

**Related
Commands**

[event](#) on page 123

show fastpath

Displays the fastpath acceleration statistics.

Syntax

```
show fastpath
show fastpath cache
```

Command Mode

Privileged EXEC

Default

NA

Usage

Use the **show fastpath** command to display the fastpath statistics, including fastpath state, packets processed, cache status, and so forth.

Use the **show fastpath cache** command to display the fastpath cache entries.

Examples

The following command displays the fastpath and fastpath cache statistics:

```
MC500# show fastpath
```

```
Fastpath status:      On
Hardware acceleration: Off
Number of accel engines: 1

Cache width:          32768
Cache depth:          8
Cache adds:            0
Cache deletes:        0
Cache flushes:        22
Cache updates:        0
Cache replaces:       0
Cache active entries: 0
Cache collisions:     0
Total packets:        196049
Eligible packets:     186087
```

```
Downstream trials:      186097
Downstream hits:        0
Upstream trials:        0
Upstream hits:          0
Hits, 1st try:          0
Hits, 2nd try:          0
Hits, Nth try:          0
```

MC500# **show fastpath cache**

Upstream Cache Entries:

Buck	E	D	Source IP	Port	Destination IP	Port	PR	Station MAC
Upstream	MAC		VLAN					
----	-	-	-----	----	-----	----	-	-----
-----			----					

Downstream Cache Entries:

Buck	E	D	Source IP	Port	Destination IP	Port	PR	Station MAC
Downstream	MAC		AP IP		Port			
----	-	-	-----	----	-----	----	-	-----
-----			-----		-----			

**Related
Commands**

fastpath on page 126

show features

Displays the installed patch features.

show fingerprints

Displays the device fingerprints stored on the system.

Syntax

show fingerprints

Command Mode

Privileged EXEC

Default

NA

Usage

Device fingerprints allow the system to detect and display the OS and type of device in use based on the device's signature. Use the **show fingerprints** command to display the device fingerprints currently configured.

Examples

```
controller# show fingerprints
ID | Option 55 Description | Hexadecimal characters
1 Apple iOS 370103060f77fc
2 Apple Mac OSX 370103060f775ffc2c2e2f
3 Cisco VoIP Phone 370103060c0f1c2a429596
4 Google Android 2.x 3701792103
5 Google Android 2.1 370103061c21333a3b79
6 Google Android 2.3.x 3701792103061c333a3b
7 Google Android JellyBean 37012103060f1c333a3b
8 Google Android 2.3.6 3701792103060f1c333a3b77
9 Blackberry OS 370103060f
10 Nokia Maemo OS 370103060c0f111c28292a
11 Microsoft Windows7-Vista 37010f03062c2e2f1f2179f92b
12 Microsoft WindowsXP 37010f03062c2e2f1f21f92b
13 Microsoft Windows Phone 7 370103060f2c2e2f
14 Symbian OS 370c060f01031c78
15 Debian/Linux 2.6 generic 37011c02030f0677
16 Linux (unknown) 37011c02030f06770c2c2f1a792a
17 Ubuntu OS 37011c02030f06770c2c2f1a792a79f9fc2a
18 Palm OS 37011c02030f060c
```

Related Commands

[fingerprint](#) on page 127

show flash

Displays the system image filenames in flash memory.

Syntax

show flash

Command Mode

Privileged EXEC

Default

NA

Usage

Use the **show flash** command to display the system image filenames in flash memory.

Examples

The following command lists the system images in flash memory:

```
controller# show flash
3.2-116
3.1-139
controller#
```

Related Commands

[delete](#) on page 77

show guest-user

Displays the captive portal guest user account information.

Syntax

show guest-user

Command Mode

Privileged EXEC

Default

NA

Usage

Use the **show guest-user** command to display the guest-user account information.

Each entry shows the name of the account, the date the account becomes active and the date the account will be deactivated.

Examples

The following command shows the guest user accounts:

```
controller# show guest-user
Guest User Name      Service Start Time      Service End Time
frieda 05/30/2008 12:00:00      05/30/2008 15:00:00
Guest User Table(1 entry)
```

Related Commands

- [guest-user on page 128](#)
- [ping on page 143](#)

show interfaces accel

Displays the accelerated Ethernet port statistics.

Syntax

```
show interfaces accel  
show interfaces accel <n>  
show interfaces accel <n> realtime
```

n The accel interface that you want to view (1, 2, etc).

Command Mode

Privileged EXEC

Default

NA

Usage

This command displays the number of the accelerated Ethernet interface cards that are installed in the MC4100. The realtime option allows you to continuously view the status.

Examples

The following command displays MC4100 accelerated card statistics:

```
mc4100# show interfaces accel
```

Related Commands

show hostname

Displays the hostname of the controller.

Syntax

show hostname

Command Mode

Privileged EXEC

Default

The default hostname is *default*.

Usage

Use the **show hostname** command to display the hostname of the controller. If you did not change the hostname, the controller hostname is *default*.

The hostname can be changed with the **setup** or **hostname** commands.

Examples

The following command displays the controller hostname, *controller*.

```
controller# show hostname
controller
controller#
```

Related Commands

- [hostname on page 130](#)
- [setup on page 161](#)

show license

Displays the system license.

Syntax `show license`

Command Mode Privileged EXEC

Default Shows the system licenses.

Usage Use the **show license** command to display the status of system licensing for all WLAN controllers and APs. The command provides the following information:

Parameter	Description
Feature Name	Displays the name of the feature being licensed (for example, controller or AP).
CtrlStatus	Shows the status of the controller entry, either the active controller, or the standby controller if a redundant configuration is implemented.
LicenseType	Show the type of license in use: temporary or permanent.
Expiry Date	Show the date a temporary license expires. The field contains '-' if the license is permanent.
TotalCount	Shows the total number of entities the license covers.
InUse	Shows the number of licensed entities that are currently being used.

Examples The following command displays a sample system license table.

forti-wifi# **show license**

Feature Name CtrlStatus LicenseType Expiry Date TotalCount InUse

controller	active	permanent	-	1	1
ap	active	permanent	-	150	0

License Table(2)

**Related
Commands**

- [copy](#) on page 73
- [license](#) on page 135
- [show license-file](#) on page 201

show ip udp-broadcast downstream all-ports

Displays the state of broadcast downstream ports.

Syntax

`show ip udp-broadcast downstream all-ports`

Command Mode

Exec Mode

Default

NA

Usage

Use this command to show whether all downstream udp-broadcast streams are **on** or **selected**. If you use the command `show ip udp-broadcast downstream all-ports` when the **selected** version of this command is active, you see a list of up to eight ports enabled by the legacy command `ip udp-broadcast downstream <portNumber>`.

Examples

This command displays the state of downstream broadcast ports:

```
default# show ip udp-broadcast downstream all-ports
Downstream UDP Broadcast All Ports
```

```
UDP All Ports : on
default#
```

Related Commands

- [show ip udp-broadcast upstream all-ports on page 199](#)
- [show ip udp-broadcast upstream-bridged all-ports on page 200](#)
- [ip udp-broadcast downstream on page 131](#)
- [ip udp-broadcast downstream-bridged on page 132](#)
- [ip udp-broadcast upstream on page 133](#)
- [ip udp-broadcast upstream-bridged on page 134](#)

show ip udp-broadcast downstream-bridged all-ports

Displays the state of broadcast downstream bridged ports.

Syntax

`show ip udp-broadcast downstream-bridged all-ports`

Command Mode

Exec Mode

Default

NA

Usage

Use this command to show whether all downstream-bridged udp-broadcast streams are **on** or **selected**. If you use the command `show ip udp-broadcast downstream-bridged all-ports` when the **selected** version of this command is active, you see a list of up to eight ports enabled by the legacy command `ip udp-broadcast downstream-bridged <port-Number>`.

Examples

This command displays the state of downstream bridged broadcast ports:

```
default# show ip udp-broadcast downstream-bridged all-ports
Downstream UDP Broadcast All Ports
```

```
UDP All Ports : on
default#
```

Related Commands

- [*show ip udp-broadcast upstream all-ports on page 199*](#)
- [*show ip udp-broadcast upstream-bridged all-ports on page 200*](#)
- [*ip udp-broadcast downstream on page 131*](#)
- [*ip udp-broadcast downstream-bridged on page 132*](#)
- [*ip udp-broadcast upstream on page 133*](#)
- [*ip udp-broadcast upstream-bridged on page 134*](#)

show ip udp-broadcast upstream all-ports

Displays the state of broadcast upstream broadcast ports.

Syntax

`show ip udp-broadcast upstream all-ports`

Command Mode

Exec Mode

Default

NA

Usage

Use this command to show whether all upstream udp-broadcast streams are **on** or **selected**. If you use the command `show ip udp-broadcast upstream all-ports` when the **selected** version of this command is active, you see a list of up to eight ports enabled by the legacy command `ip udp-broadcast upstream <portNumber>`.

Examples

This command displays the state of upstream broadcast of all ports:

```
default# show ip udp-broadcast upstream all-ports
```

```
Upstream UDP Broadcast All Ports
```

```
UDP All Ports : on
```

```
default#
```

Related Commands

- [*show ip udp-broadcast downstream all-ports*](#) **on page 197**
- [*show ip udp-broadcast downstream-bridged all-ports*](#) **on page 198**
- [*ip udp-broadcast downstream*](#) **on page 131**
- [*ip udp-broadcast downstream-bridged*](#) **on page 132**
- [*ip udp-broadcast upstream*](#) **on page 133**
- [*ip udp-broadcast upstream-bridged*](#) **on page 134**

show ip udp-broadcast upstream-bridged all-ports

Displays the state of broadcast upstream bridged broadcast ports.

Syntax

`show ip udp-broadcast upstream-bridged all-ports`

Command Mode

Exec Mode

Default

NA

Usage

Use this command to show whether all upstream-bridged udp-broadcast streams are **on** or **selected**. If you use the command **show ip udp-broadcast upstream-bridged all-ports** when the **selected** version of this command is active, you see a list of up to eight ports enabled by the legacy command **ip udp-broadcast upstream-bridged <portNumber>**.

Examples

This command displays the state of upstream broadcast of all ports:

```
default# show ip udp-broadcast upstream-bridged all-ports
Upstream UDP Broadcast All Ports
```

```
UDP All Ports : on
default#
```

Related Commands

- [show ip udp-broadcast downstream all-ports on page 197](#)
- [show ip udp-broadcast downstream-bridged all-ports on page 198](#)
- [ip udp-broadcast downstream on page 131](#)
- [ip udp-broadcast downstream-bridged on page 132](#)
- [ip udp-broadcast upstream on page 133](#)
- [ip udp-broadcast upstream-bridged on page 134](#)

show license-file

Displays the content of system license files.

Syntax

show license-file Command Mode

Privileged EXEC

Default

NA

Usage

Use the **show license-file** command to show the detailed content of the active or standby controller license. The output will also list the licensed features.

Examples

The following example shows the content of the active controller license:

```
slave# show license-file

----- STANDALONE LICENSE -----

SERVER this_host ANY
VENDOR Fortinetd
USE_SERVER
INCREMENT controller fortid 1.0 permanent 1 \
    HOSTID=COMPOSITE=2F402A47C8FE ISSUED=19-mar-2007 \
    START=16-jan-2007 SIGN="00E5 BBB3 2865 4C8C A6C0 57E9 B12F \
    1F00 4F91 ED66 12BB 7009 924B 8337 FD9C"
INCREMENT ap fortid 1.0 permanent 150 HOSTID=COMPOSITE=2F402A47C8FE \
    ISSUED=19-mar-2007 START=16-jan-2007 SIGN="0082 37BB 8DB1 F8C3 \
    D379 5691 D6C3 2400 7C79 45EC BF94 427A 1507 FC9B A583"
```

Related Commands

- [license](#) on page 135
- [show license](#) on page 195

show log

Displays the system logs.

Syntax

`show log [running-config]`

Command Mode

Privileged EXEC

Default

Displays the system logs.

Usage

Use the **show log** command to display the controller system log. Using the optional keyword **running-config**, shows the log for the running configuration only. In release 4.1, this command was enhanced to display configuration changes (CLI or GUI), key commands, events and operations, and errors.

Examples

The following are a few lines from the controller log, which is usually very long.

```
forti-wifi# show log
Aug  8 09:46:19 forti-wifi ALARM: AP DOWN CRITICAL Access Point #10-1F-Mktg-208 (10) at location Near printer
Aug  8 09:46:19 forti-wifi ALARM: 11235195791 | system | info | ALR | AP DOWN CRITICAL Access Point #10-1F-Mktg-208 (10) at location Near printer
Aug  8 09:46:22 forti-wifi ALARM: AP UP Access Point #10-1F-Mktg-208 (10) is up
Aug  8 09:46:22 forti-wifi ALARM: 11235195821 | system | info | ALR | AP UP Access Point #10-1F-Mktg-208 (10) is up
Aug  8 13:42:34 forti-wifi ALARM: AP DOWN CRITICAL Access Point #10-1F-Mktg-208 (10) at location Near printer
```

Related Commands

- [show running-config on page 90](#)
- [syslog-host on page 228](#)

show nms-server

Displays the IP address of the E(z)rf Network Manager Service Appliance for a controller, along with the E(z)RF version and connectivity status.

Syntax

show nms-server

Command Mode

Privileged EXEC

Default

NA

Usage

Use this command to see a controller’s Server ID, Server IP, Controller ID in Network Manager, Network Manager version on the service appliance, and the connection status to Network Manager.

Examples

This example displays the Network Manager information for a controller:

corpwifi# sh nms-server

Server ID	Server IP	Controller ID	NmsAgent Version	Server connectivity status
1	192.168.34.210	5	2.1-4.0-A-98	connected

Related Commands

show ntp-server

Shows the assigned Network Time Protocol (NTP) server.

Syntax

show ntp-server

Command Mode

Privileged EXEC

Default

NA

Usage

Use the **show ntp-server** command to show the NTP server that has been specified with the **ntp server** command.

Examples

The following command shows the NTP server:

```
MC4200-1(15)# show ntp-server
NTP updates are enabled.
Server: asia.pool.ntp.org
```

Related Commands

[ntp](#) on page 141

show roaming-domain

Shows the status of the roaming-domain configuration.

Syntax

```
show roaming-domain
show roaming-domain all
```

Command Mode

Privileged EXEC

Default

NA

Usage

Use the **show roaming-domain** command to show the status of the ICR roaming-domain group that has been specified with the **roaming-domain** command. Use the **all** argument to show the verbose display.

Examples

The following command shows the roaming-domain status:

```
MC500# show roaming-domain
Roaming domain configuration:
```

```
Controller 192.168.1.100
Controller 192.168.2.101
```

Roaming domain is active.

The following uses the **all** argument and shows the verbose version:

```
MC500# show roaming-domain all
Roaming domain configuration:
```

```
Controller 192.168.1.100
Controller 192.168.2.101
```

Roaming domain is active. Running Status:

```
[05/23 07:48:042] Roaming state:
```

My Interface Addresses:

VLAN	IP	Netmask	MAC	Device IP
Gw				
0	192.168.1.30	255.255.255.0	00:02:b6:35:33:d2	native
	192.168.1.30			

Peer Controllers:

IP	Tunnel IP	VLAN
192.168.1.100	10.235.0.1	-1
192.168.2.101	10.235.0.2	-1

**Related
Commands**

[roaming-domain](#) on page 158

show syslog-file

Displays the external syslog file, if it exists.

Syntax

```
show syslog-file
show syslog-file <facility>
```

facility The optional facility parameter filters the output to show entries for that facility only. Possible entries for *facility* are:

- 802.mobility
- bulkupdate
- nms
- qos
- security
- system

Command Mode

Privileged EXEC

Default

NA

Usage

This command shows the contents of the external syslog file, if it exists. By default, external logging is disabled. You can configure an external syslog host with the **syslog-host** command.

Examples

The following command shows the syslog file upgrade module:

```
controller# show syslog-file upgrade
```

Line	Priority	Mnemonic	Time	Record
1	info	UPG	2008/01/17 00:43:12	Upgrade AP(s) from:3.6-6 to:3.6-6
2	info	UPG	2008/01/17 00:43:12	Upgrade AP 1 START
3	info	UPG	2008/01/17 00:43:12	Upgrade AP 2 START
4	info	UPG	2008/01/17 00:43:12	Upgrade AP 1 Upgrade Requested

5	info	UPG	2008/01/17 00:43:12	Upgrade AP 2 Upgrade Requested
6	info	UPG	2008/01/17 00:43:13	Upgrade AP 1 Reading File
7	info	UPG	2008/01/17 00:43:13	Upgrade AP 2 Reboot Requested
8	info	UPG	2008/01/17 00:43:15	Upgrade AP 1 Verifying Checksum
9	info	UPG	2008/01/17 00:43:16	Upgrade AP 1 Erasing Flash
10	info	UPG	2008/01/17 00:43:21	Upgrade AP 1 Writing Flash
11	info	UPG	2008/01/17 00:43:37	Upgrade AP 1 Success
SysLog(11 entries)				

**Related
Commands**

[syslog-host](#) on page 228

show syslog-host

Displays the external syslog host if it is configured.

Syntax `show syslog-host`

Command Mode Privileged EXEC

Default NA

Usage By default, external logging is disabled. You can configure an external syslog host with the **syslog-host** command.

Examples The following command shows the syslog host is 10.1.2.3:

```
controller(config)# show syslog-host
10.1.2.3
controller(config)#
```

- Related Commands**
- [syslog-host](#) on page 228
 - [show syslog-file](#) on page 207
 - [show syslog-table](#) on page 210

show syslog-table

Displays the external syslog facility table.

Syntax

```
show syslog-table
show syslog-table <facility>
```

facility The optional facility parameter filters the output to show entries for that facility only. Possible entries for *facility* are:

- 802.mobility
- bulkupdate
- nms
- qos
- security
- system

Command Mode

EXEC

Default

NA

Usage

This command shows the contents of the external syslog table, if it exists. By default, external logging is disabled. You can configure an external syslog host with the **syslog-host** command.

Examples

```
controller# show syslog-table
Description          Last Accessed Size      # Lines Last Record

Security             2008/03/06 14:21:55      2         0
QoS                  2008/03/06 14:21:47      1         0
System WNC           2008/03/06 14:21:54      1         0
NMS                  2008/03/06 14:21:47      1         0
Mobility             2008/03/06 14:21:47      1         0
Bulk Update          2008/03/06 14:21:47      1         0
Upgrade              2008/03/06 14:15:52      1         0
Per User Firewall    2008/03/06 14:22:02      1         0
```

The following command shows the syslog file has no entries, although it does exist:

```
controller(config)# show syslog-table security
```

Line	Priority	Mnemonic	Time	Record
31	info	WAU	2005/08/05 10:37:27	admin@10.0.220.25
logged in OK				
SysLog(1 entry)				

```
controller(config)#
```

Related Commands

- [show syslog-file](#) on page 207
- [show syslog-host](#) on page 209

show sys-summary

Displays various statistics about the system status, depending on the parameter provided.

Syntax

show sys-summary <ess/general/resources/stations/throughput>

ess	Displays information on a per-ESS basis.
general	Displays general details about the system.
resources	Displays CPU, filesystem, and memory statistics for the system.
stations	Displays statistics relating to the number and types of stations currently connected.
<i>throughput</i>	Displays assorted throughput statistics for the controller.

Command Mode

Privileged EXEC

Default

NA

Usage

The **show sys-summary** command allows the user to view detailed statistics about the wireless environment and the controller itself. Each parameter provides for a different information listing.

Examples

This example displays the output from the **resources** parameter.

```
default(15)# show sys-summary resources
System Resources Status
CPU Usage User[%] : 0
CPU Usage System[%] : 0
CPU Usage Idle[%] : 99
Memory Size Total[K] : 4008008
Memory Size Used[K] : 244100
Memory Size Free[K] : 3763908
Root File System Size Total[K] : 897363
Root File System Size Used[K] : 566296
Root File System Size Available[K] : 283190
```



```
Root File System Usage[%] : 67
default(15)#
```

Related Commands

- [*show sys-summary ess*](#) **on page 214**
- [*show sys-summary general*](#) **on page 216**
- [*show sys-summary resources*](#) **on page 218**
- [*show sys-summary stations*](#) **on page 219**
- [*show sys-summary throughput*](#) **on page 220**

show sys-summary ess

Displays various statistics about all ESSIDs configured or about a specific ESS, as desired.

Syntax

show sys-summary ess <ess>

ess Specify the desired ESS for specific details.

Command Mode

Privileged EXEC

Default

NA

Usage

This version of the **show sys-summary** command allows for two options:

- **show sys-summary ess:** Lists all ESSIDs and details about their transmit and receive values.
- **show sys-summary ess <ess>:** Lists specific details about the specified ESS.

Both versions of the command provide the following details:

- RF Band—The band(s) on which the ESS operates.
- Radios—The number of radios allocated to each ESS.
- RX_TP—The throughput rate for receiving (in bits per second).
- TX_TP—The throughput rate for transmitting (in bits per second).
- Total_TP—The overall throughput (combined transmit and receive in bits per second).
- Stations—The total number of stations on each band for the ESS.

Examples

This example displays the output from both the general and specific version of the command.

```
Default(15)# show sys-summary ess
ESSID RFBAND RADIOS RX_TP[bps] TX_TP[bps] TOTAL_TP[bps] STATIONS
vcellclear 2.4GHz 4 0 0 0 1
vcellclear 5GHz 5 0 0 0 3
vcellmixedpsk 2.4GHz 4 0 0 0 0
```

```

vcellmixedpsk 5GHz 3 0 0 0 0
vcellwep64 2.4GHz 4 0 0 0 0
vcellwep64 5GHz 4 0 0 0 0
vcellwpa 2.4GHz 4 0 0 0 0
vcellwpa 5GHz 4 0 0 0 0
vcellwpa2 2.4GHz 3 0 0 0 0
vcellwpa2 5GHz 4 0 0 0 0
vcellwpa2psk 2.4GHz 5 0 0 0 4
vcellwpa2psk 5GHz 5 149 0 149 15
vcellwpapsk 2.4GHz 5 30 0 30 1
vcellwpapsk 5GHz 5 39 0 39 4
ESS Statistics Summary(14 entries)

```

```

default15)# show sys-summary ess vcellwpa2psk
RFBAND RADIOS RX_TP[bps] TX_TP[bps] TOTAL_TP[bps] STATIONS
2.4GHz 5 0 0 0 4
5GHz 5 149 0 149 15
ESS Statistics Summary(2 entries)
default(15)#

```

Related Commands

- [show sys-summary on page 212](#)
- [show sys-summary general on page 216](#)
- [show sys-summary resources on page 218](#)
- [show sys-summary stations on page 219](#)
- [show sys-summary throughput on page 220](#)

show sys-summary general

Displays general details about the controller and FortiWLC (SD) status.

Syntax

show sys-summary general

Command Mode

Privileged EXEC

Default

NA

Usage

This version of the **show sys-summary** command allows the user to view detailed information about the controller configuration and general statistics about the wireless devices serviced by it. This information includes:

- Controller Hostname
- Controller Model
- Software Version
- Total number of installed, allowed, online, and offline APs
- Total number of wired and wireless stations
- Total number of alarms, separated by severity

Additional details are also provided as supported by the controller.

Examples

```
default(15)# show sys-summary general
System General Information
Controller's Hostname : Engg-wifi-Main-4200
Controller's Model Name : MC4200
Controller's Version : 5.2-32
Controller's Uptime : 01d:23h:02m:49s
Access Point Limit : 500
Client(s) : 5000
Installed Access Point License Count : 150
In-Use Access Point License Count : 5
Online Access Point Count : 5
Offline Access Point Count : 1
```

Wireless Station Count : 24
2.4GHz Station Count : 6
5GHz Station Count : 18
Wired Station Count : 0
Alarm Count : 10
Critical Alarm Count : 5
Major Alarm Count : 0
Minor Alarm Count : 5
Rogue Access Point Count : 0
Rogue Station Count : 0
Unknown Rogue Device Count : 0
Clear ESS Profile Count : 1
Secure ESS Profile Count : 7
Captive Portal ESS Profile Count : 2
default(15)#

Related Commands

- [*show sys-summary*](#) **on page 212**
- [*show sys-summary ess*](#) **on page 214**
- [*show sys-summary resources*](#) **on page 218**
- [*show sys-summary stations*](#) **on page 219**
- [*show sys-summary throughput*](#) **on page 220**

show sys-summary resources

Displays statistics relating to the controller's resource status.

Syntax

show sys-summary resources

Command Mode

Privileged EXEC

Default

NA

Usage

This version of the **show sys-summary** command allows the user to view detailed information about the controller's resource status, including CPU usage, memory consumption, and free disk space.

Examples

```
default(15)# show sys-summary resources
System Resources Status
CPU Usage User[%] : 0
CPU Usage System[%] : 0
CPU Usage Idle[%] : 99
Memory Size Total[K] : 4008008
Memory Size Used[K] : 250704
Memory Size Free[K] : 3757304
Root File System Size Total[K] : 897363
Root File System Size Used[K] : 566296
Root File System Size Available[K] : 283190
Root File System Usage[%] : 67
default(15)#
```

Related Commands

- [show sys-summary on page 212](#)
- [show sys-summary ess on page 214](#)
- [show sys-summary general on page 216](#)
- [show sys-summary stations on page 219](#)
- [show sys-summary throughput on page 220](#)

show sys-summary stations

Displays statistics relating to the stations actively serviced by the controller.

Syntax

show sys-summary stations

Command Mode

Privileged EXEC

Default

NA

Usage

This version of the **show sys-summary** command allows the user to view detailed information about the number and type of stations currently present on the network. This information is divided by band, number of data streams used, and type of station (data or phone).

Examples

```
default(15)# show sys-summary stations
System Stations Status
802.11a Station Count : 8
802.11an1stream Station Count : 0
802.11an2stream Station Count : 12
802.11an3stream Station Count : 0
802.11b Station Count : 0
802.11bg Station Count : 0
802.11gn1stream Station Count : 0
802.11gn2stream Station Count : 2
802.11gn3stream Station Count : 0
Associated Data Station Count : 20
Associated Phone Station Count : 1
default(15)#
```

Related Commands

- [show sys-summary on page 212](#)
- [show sys-summary ess on page 214](#)
- [show sys-summary general on page 216](#)
- [show sys-summary resources on page 218](#)
- [show sys-summary throughput on page 220](#)

show sys-summary throughput

Displays statistics relating to the throughput levels in the wireless network.

Syntax

show sys-summary throughput

Command Mode

Privileged EXEC

Default

NA

Usage

This version of the **show sys-summary** command allows the user to view detailed information about the throughput levels experienced in the current wireless environment. These details are divided by receiving (Rx) and transmitting (Tx) levels and are shown in bits per second (bps).

Examples

```
default(15)# show sys-summary throughput
System Throughput Information
Controller Total Rx Bytes : 23858571
Controller Total Tx Bytes : 23833005
Controller Rx Throughput[bps] : 3181142
Controller Tx Throughput[bps] : 3177734
WLAN Total Rx Bytes : 896675
WLAN Total Tx Bytes : 34319495
WLAN Rx Throughput[bps] : 119556
WLAN Tx Throughput[bps] : 4575932
default(15)#
```

Related Commands

- [show sys-summary on page 212](#)
- [show sys-summary ess on page 214](#)
- [show sys-summary general on page 216](#)
- [show sys-summary resources on page 218](#)
- [show sys-summary stations on page 219](#)

show system-id

Displays a controller's System ID that is needed for license generation.

Syntax `show system-id`

Command Mode Privileged EXEC

Default NA

Usage

Examples This command displays the controller ID needed to apply for a license.

```
Master# show system-id
System Id : COMPOSITE=272FF2EEB5F8
Master#
```

Related Commands [*license*](#) on page 135

show timezones

Displays timezones and related cities.

Syntax

show timezones

Command Mode

Privileged EXEC

Default

NA

Usage

This command shows a listing a major cities, categorized by timezone.

Examples

The following shows a partial list of the command output:

```
controller(config)# show timezones
Africa/Abidjan
Africa/Accra
Africa/Addis_Ababa
Africa/Algiers
Africa/Asmera
Africa/Bamako
Africa/Bangui
Africa/Banjul
Africa/Bissau
Africa/Blantyre
Africa/Brazzaville
Africa/Bujumbura
Africa/Cairo
Africa/Casablanca
.
.
.
```

Related Commands

[*timezone*](#) on page 230

spectrum-band

Enables and disables spectrum scanning on particular portions of the wireless environment.

Syntax

```
spectrum-band [band]  
no spectrum-band [band]
```

Command Mode

Global configuration

Default

NA

Usage

This command allows the user to fine-tune the portions of the wireless spectrum to be scanned for spectrum analysis. The **no** form of the command disables the specified band. The command can be repeated to enable it on multiple portions of the spectrum, or simply use the **all** parameter to scan the entire spectrum.

Examples

```
controller(15)(config)# spectrum-band 2.4GHz
```

```
controller(15)(config)#
```

```
controller(15)(config)# no spectrum-band 2.4GHz
```

Related Commands

start-ntp

Starts automatic system time synchronizing of the system clock with a specified Network Time Protocol (NTP) server.

Syntax

start-ntp

Command Mode

Privileged EXEC

Default

NA

Usage

Use the **start-ntp** command to enable automatic synchronization of the system clock with the NTP server specified with the **ntp server** command. Information about public NTP servers can be found at www.ntp.org.

Examples

To set up automatic NTP server synchronization, use the **start-ntp** command:

```
controller# start-ntp
```

Related Commands

[ntp](#) on page 141

statistics period

Configures how often the controller polls for information.

Syntax

statistics period <period>

period Amount of time that elapses before the controller polls for information. The valid value range is 5 through 65,535 seconds.

Command Mode

Global configuration

Default

The default statistics period is 60 seconds.

Usage

Use the **statistics period** command to change the amount of time that elapses before the controller polls for information. For example, by default, the controller polls for information, such as the number of packets passed or dropped, every 60 seconds. Specifying a value of zero (0) disables polling. The statistics period affects the data collected for the following commands:

- **show statistics station-per-ap**—Displays the list of station statistics per AP.
- **show statistics top10-ap-problem**—Displays the list of APs having the most significant problems.
- **show statistics top10-ap-talker**—Displays the list of APs handling the heaviest traffic (MAX Tx+Rx frames).
- **show statistics top10-station-problem**—Displays the list of stations having the most significant problems.
- **show statistics top10-station-talker**—Displays the list of stations generating the highest traffic.

Examples

The following command sets the statistics period to 1,000 seconds:

```
controller(config)# statistics period 1000
controller(config)#
```

Sysconfig backup

Performs the backup of system configuration files.

Syntax `Sysconfig backup`

Command Mode Global configuration

Default None

Usage Use this command to backup system configuration files.

Examples MC3200(15)#
MC3200(15)# configure terminal
MC3200(15)(config)# Sysconfig backup

Related Commands [Sysconfig restore](#) on page 227

Sysconfig restore

Performs restoration of system configuration files.

Syntax `Sysconfig restore`

Command Mode Global configuration

Default None

Usage Use this command to restore system configuration files.

Examples MC3200(15)#
MC3200(15)# configure terminal
MC3200(15)(config)# Sysconfig restore

Related Commands [Sysconfig backup](#) on page 226

syslog-host

Configures an external syslog host.

Syntax

```
syslog-host <hostname>  
no syslog-host
```

hostname Name or IP address, in dotted decimal notation, of the external syslog host.

Command Mode

Global configuration

Default

By default, no host is specified.

Usage

This command configures a remote server to serve as the location where the syslog error logging file is maintained. By default, no host is specified. To remove a configured syslog server, use the **no syslog-host** command.

Examples

The following commands check the syslog host setting, set host 10.1.2.3 to the external syslog server, and then display the change:

```
controller(config)# do show syslog-host  
External logging is disabled  
controller(config)# syslog-host 10.1.2.3  
controller(config)# do show syslog-host  
10.1.2.3
```

The following commands remove the syslog host setting and then display the change:

```
controller(config)# no syslog-host  
controller(config)# do show syslog-host  
External logging is disabled
```

Related Commands

[show syslog-host](#) on page 209

telnet

Configure telnet connectivity.

Syntax

```
telnet enable  
telnet disable
```

Command Mode

Global configuration mode

Default

Telnet access is disabled.

Usage

This command disables telnet access to the controller when telnet is enabled, or enables access if telnet is disabled.

Examples

The following command disables telnet access:

```
controller(config)# telnet disable
```

timezone

Configures the timezone setting.

Syntax

```
timezone menu
timezone set <zone>
```

zone Directly sets the timezone to a specific setting.

Command Mode

Privileged EXEC mode

Default

NA

Usage

This command configures the timezone setting for the controller. The **menu** option presents a menu containing a series of numbered lists of locations (continents and oceans), and the timezone is set by selecting a location. At the end of the selection questions, you are prompted to set the timezone, and notified of the zone setting. The *zone* setting can be used in subsequent timezone sessions, as an argument to the **set** option. After the timezone is changed, the controller must be rebooted.

Examples

The following shows how to set the timezone using the **menu** option:

```
controller(config)# timezone menu
Please identify a location so that time zone rules can be set correctly.
Please select a continent or ocean.
 1) Africa
 2) Americas
 3) Antarctica
 4) Arctic Ocean
 5) Asia
 6) Atlantic Ocean
 7) Australia
 8) Europe
 9) Indian Ocean
10) Pacific Ocean
```

11) none - I want to specify the time zone using the Posix TZ format.

#? 10

Please select a country.

- | | |
|---------------------|-------------------------------|
| 1) Chile | 15) Northern Mariana Islands |
| 2) Cook Islands | 16) Palau |
| 3) Ecuador | 17) Papua New Guinea |
| 4) Fiji | 18) Pitcairn |
| 5) French Polynesia | 19) Samoa (American) |
| 6) Guam | 20) Samoa (Western) |
| 7) Kiribati | 21) Solomon Islands |
| 8) Marshall Islands | 22) Tokelau |
| 9) Micronesia | 23) Tonga |
| 10) Nauru | 24) Tuvalu |
| 11) New Caledonia | 25) US minor outlying islands |
| 12) New Zealand | 26) United States |
| 13) Niue | 27) Vanuatu |
| 14) Norfolk Island | 28) Wallis & Futuna |

#? 26

Please select one of the following time zone regions.

- 1) Eastern Time
- 2) Eastern Time - Michigan - most locations
- 3) Eastern Time - Kentucky - Louisville area
- 4) Eastern Time - Kentucky - Wayne County
- 5) Eastern Standard Time - Indiana - most locations
- 6) Eastern Standard Time - Indiana - Crawford County
- 7) Eastern Standard Time - Indiana - Starke County
- 8) Eastern Standard Time - Indiana - Switzerland County
- 9) Central Time
- 10) Central Time - Michigan - Wisconsin border
- 11) Central Time - North Dakota - Oliver County
- 12) Mountain Time
- 13) Mountain Time - south Idaho & east Oregon
- 14) Mountain Time - Navajo
- 15) Mountain Standard Time - Arizona
- 16) Pacific Time
- 17) Alaska Time
- 18) Alaska Time - Alaska panhandle

19) Alaska Time - Alaska panhandle neck

20) Alaska Time - west Alaska

21) Aleutian Islands

22) Hawaii

#? 16

The following information has been given:

United States

Pacific Time

The name of the time zone is 'America/Los_Angeles'.

Is the above information OK?

1) Yes

2) No

#? 1

The following command is the alternative way of selecting the same time zone

timezone set America/Los_Angeles

The time zone is successfully set

topo-update

Enables and disables the Topology Information Update feature.

The Topology Information Update is useful for troubleshooting and collecting debug information. It is recommended that you enable this feature only if you need to collect troubleshooting and debug information.

Syntax

```
topo-update enable  
topo-update disable
```

Command Mode

Global Configuration

Default

The default setting is **disable**.

Usage

This command determines whether the Topology Information Update feature is enabled or disabled. When enabled, the controller collects the troubleshooting and debug information that is used for the topology-related **show** commands (**show topoap**, **show topoapap**, **show topostaap**, **show topostation**).

Gathering of the topo information is disabled by default.

Examples

Gathering of the topo information is disabled by default. To enable topo gathering, use this command:

```
barneveld# configure terminal  
barneveld(config)# topo-update enable  
barneveld(config)# exit
```

traceroute

Tests network connectivity.

Syntax

traceroute <hostname>

hostname Name or IP address, in dotted decimal notation, of the host address to resolve.

Command Mode

Privileged EXEC

Default

NA

Usage

This command displays the IP address and status for all routers between the controller and a specified remote destination. Instead of a hostname, you can alternatively specify a domain name instead of an IP address or a hostname.

Examples

The following command displays the route to a destination whose hostname is Ourserver:

```
controller# traceroute Ourserver
traceroute to OurServer (10.0.13.1), 30 hops max, 38 byte packets
 1  mc3000 (10.19.1.1)  2997.354 ms !H  2999.525 ms !H  2999.944 ms !
```

Related Commands

[ping](#) on page 143

zeronet-packet

Enables/disables forwarding of IPv4 unicast packets whose source/destination IP address begins with 0 (zeronet) except 0.0.0.0.

Syntax

```
zeronet-packet enable  
zeronet-packet disable
```

Command Mode

Global Configuration

Default

Disabled

Usage

This feature enables and disables the forwarding of IPv4 unicast packets whose source or destination IP address begins with 0 (zeronet) except for ther address 0.0.0.0.

Example

```
amecntrl# configure terminal  
ramecntrl(config)# zeronet-packet ?  
<value>                               Enter Enable or Disable for Zeronet configuration  
    disable                            Disable  
    enable                             Enable  
ramecntrl(config)# zeronet-packet enable  
ramecntrl(config)# zeronet-packet disable  
ramecntrl(config)# exit
```


6 Redundancy Commands

This chapter describes the commands used to configure the N+1 redundancy features that are available for protecting the system availability. You can either use the **nplus1** commands shown here to set up one or more master controllers with one backup standby controller, or you can configure Option 43 from the Web UI.

The nplus1 commands include the following:

- [*nplus1 add on page 238*](#)
- [*nplus1 add on page 238*](#)
- [*nplus1 delete on page 240*](#)
- [*nplus1 disable on page 241*](#)
- [*nplus1 enable on page 242*](#)
- [*nplus1 revert on page 244*](#)
-
- [*nplus1 setdebugloglevel on page 246*](#)
- [*nplus1 start master on page 247*](#)
- [*nplus1 start slave on page 248*](#)
- [*nplus1 stop on page 250*](#)
- [*nplus1 timeout on page 252*](#)
- [*show nplus1 on page 253*](#)
- [*show nplus1 debugloglevel on page 257*](#)

nplus1 add

Adds a master controller to the slave's cluster list.

Syntax

```
nplus1 add <master_hostname> <master_ip-address>
```

master_hostname Hostname of master controller.

master_ip-address IP address of master controller.

Command Mode

Global Configuration

Default

NA

Usage

The **nplus1 add** command is used on a standby slave controller and adds the master controllers that the slave will monitor.

Before beginning an N+1 configuration, disable any active High Availability (HA) service on all cluster controllers (use **high-availability stop**). Additionally, start N+1 on the slave and all masters (using **nplus1 start slave** and **nplus1 start master**) before using this command.

Use the **nplus1 add** command to add up to 5 master controllers to one backup slave controller, adding one master at a time. Supply the hostname (for example, 3000-1) and IP address of each master controller in the cluster. You will be prompted for the controller's password to complete the addition.

If you are replacing an existing controller, after executing the **nplus1 add master** command, execute the **nplus1 access** command.

Examples

The following commands add the master controller named 3000-1 with the IP address 10.1.1.10 to the cluster list of the backup slave controller 3000-slave, then enable access for that master controller using its IP address 10.1.1.10.

```
3000-slave(config)# nplus1 add 3000-1 10.1.1.10
admin@10.1.1.10 Password: xxx
3000-slave(config)# nplus1 access 10.1.1.10
```

Related Commands

- [*nplus1 start master*](#) on page 247
- [*nplus1 start slave*](#) on page 248
- [*show nplus1*](#) on page 253

nplus1 delete

Removes an N+1 master controller from the cluster.

Syntax

nplus1 delete <master_ip-address>

master_ip-address IP address of master controller.

Command Mode

Global Configuration

Default

NA

Usage

To remove an N+1 master controller from the slave's cluster, issue the **nplus1 delete** command from the slave controller. **nplus1 delete** works only on a standby slave controller.

Example

The following command deletes the master controller with IP address 10.1.1.10 from the slave controller 3000-slave.

```
3000-slave(config)# nplus1 delete 10.1.1.10
```

Related Commands

[show nplus1](#) on page 253

nplus1 disable

Disables N+1 operation on a master controller.

Syntax

nplus1 disable <master_ip-address>

master_ip-address IP address of master controller.

Command Mode

Global Configuration

Default

NA

Usage

To disable N+1 operation on a master controller, but still maintain its configuration in the cluster, issue the **nplus1 disable** command from the slave controller. To issue **nplus1 disable**, the slave must be in the standby state, and not switched to active slave (replacing a master controller).

To restore a master controller, issue the **nplus1 enable** command from the slave controller.

Example

This example disables the master controller with IP address 10.1.1.10 from the slave controller named 3000-slave:

```
3000-slave(config)# nplus1 disable 10.1.1.10
```

Related Commands

- [nplus1 enable on page 242](#)
- [show nplus1 on page 253](#)

nplus1 enable

Restores the master controller status after **nplus1 disable**.

Syntax

nplus1 enable <master_ip-address>

master_ip_address IP address of master controller.

Command Mode

Global Configuration

Default

NA

Usage

Use this command to enable N+1 operation on a master controller that had been disabled.

To allow access the newly enabled master controller, issue the **nplus1 access** command from the slave controller.

Example

This example enables a master controller with IP address 10.1.1.10 from the slave controller named 3000-slave:

```
3000-slave(config)# nplus1 enable 10.1.1.10
```

Related Commands

- [nplus1 add on page 238](#)
- [nplus1 disable on page 241](#)
- [show nplus1 on page 253](#)

nplus1 period

Changes the heartbeat period in the slave controller.

Syntax

nplus1 period <hb_period>

duration

The duration is time in seconds during which the slave will send advertisements to the master controller.

Values are between 100 and 30000.

Command Mode

Global Configuration

Default

1000 seconds

Usage

Use the **nplus1 period** command in the slave controller to change the heartbeat duration to send advertisements to the master controller. If the slave controller does not receive advertisements from the master, auto failover is initiated.

After a failover, the master (passive) will monitor advertisements from active slave. If the master does not receive advertisements within the time period, auto fallback is initiated.

Example

This example changes the heartbeat period to 2000 seconds

```
NP1-MC4200-slave(15)(config)# nplus1 period 2000
nplus1 period set: 2000 millisecond
```

Related Commands

nplus1 revert

Changes the status of the slave from active to standby.

Syntax

nplus1 revert

Command Mode

Global Configuration

Default

NA

Usage

Use the **nplus1 revert** command to change the status of the slave controller from active (replacing one of the master controllers) back to standby. Use this command if it becomes obvious the failed controller is to be offline for some time and should be replaced. By reverting the slave from active to standby, the rest of the cluster will continue to be monitored.

When a non-revertive mode is enabled, the master controller must be up for **nplus1 revert** to work on Active slave controller.

If master controller is down and if **nplus1 revert** command is issued, revert will not happen.

In this case, if revert has to be done,

Use the command **nplus1 revert force** to change the state from Active slave to Passive.

For Example:

```
3000-slave# conf terminal
3000-slave(config)# nplus1 revert force
```

Example

This example changes the status of the slave 3000-slave from active back to standby:

```
3000-slave# nplus1 revert
```

Related Commands

[show nplus1](#) on page 253

nplus1 autorevert

The active slave controller triggers a fallback by itself.

Syntax `nplus1 autorevert`

Command Mode Global Configuration

Default NA

Usage When the master controller goes down, the slave controller takes over as the active slave controller. Until now, when the master controller that was down became active, it continues to stay as passive controller till the nplus1 revert command was executed on the active slave controller. This behavior is now enhanced (automated) to allow auto revert after the master controller is online

Example This example enables automatically triggers fallback of the of the active slave 3000-slave:

```
3000-slave# nplus1 autorevert enable
```

Related Commands [show nplus1](#) **on page 253**

nplus1 setdebugloglevel

Sets the level of verbosity for the N+1 log messages.

Syntax

nplus1 setdebugloglevel <number>

number

The level can be set from 0 to 3, where 1 is the least verbose.
The default 0 setting disables syslog messaging.

Command Mode

Global Configuration

Default

The default is 0, syslog messaging disabled.

Usage

The **nplus1 setdebugloglevel** command sets the level of verbosity for the N+1 log messages. This command only works on a slave controller. Use the **show nplus1 debugloglevel** command to check the log setting.

Example

This example sets the log level of verboseness to 1 for the slave controller 3000-slave:

```
3000-slave(config)# nplus1 setdebugloglevel 1
```

Related Commands

- [show nplus1 on page 253](#)
- [show nplus1 debugloglevel on page 257](#)

nplus1 start master

Activates a controller as an Nplus1 master.

Syntax

nplus1 start master

Command Mode

Global Configuration

Default

NA

Usage

Execute **nplus1 start master** on all master controllers before starting the slave controller with **nplus1 start slave**. The slave controller must be the last controller in the cluster to start N+1. All master controllers must be added to the cluster before starting N+1 on the slave controller.

Examples

This example starts the master controller named 3000-master:

```
3000-master(config)# nplus1 start master
```

Related Commands

- [nplus1 start slave on page 248](#)
- [show nplus1 on page 253](#)

nplus1 start slave

Starts the N+1 slave controller.

Syntax

nplus1 start slave

Command Mode

Global Configuration

Default

NA

Usage

Start the N+1 slave controller with **nplus1 start slave** only after all N+1 master controllers are started with the command **nplus1 start master**. The standby slave then monitors the availability of the master controllers in the cluster by receiving advertisement messages sent by the masters over a UDP port at expected intervals. If five successive advertisements are not received, the standby slave changes state to an active slave, assumes the IP address of the failed master, and takes over operations for the failed master. As the standby slave has a copy of the master's latest saved configuration, all configured services continue with only a short pause while the slave switches from standby to active state.

While configuring your network for N+1 redundancy, the following guidelines must be followed:

- In the N+1 cluster, the slave and master controllers must be the same model and run the same version of FortiWLC (SD) software. A check is performed by the slave controller after each master controller is assigned to it to ensure the hardware model and FortiWLC (SD) version are identical; if a mismatch occurs, the slave is not allowed to switch over for this master, and that status is noted in the Status display for the Master Controller.
- All master and slave controllers must use static IP addressing to ensure consistency and control of N+1 clustering. (DHCP addresses are not supported for controllers participating in the N+1 cluster).
- Master and slave controllers must be on the same IP subnet.
- All APs in the network should be configured for Layer 3 connectivity with the controller.
- Spanning tree should be disabled on the switch port to which the controllers are connected. To disable spanning tree on the port, refer to your switch configuration documentation.

Note that changing from redundant to dual active configuration requires a controller reboot.

Examples

This example starts the slave controller named 3000-slave:

```
3000-slave(config)# nplus1 start slave
```

Setting up this controller as a Passive Slave controller

```
3000-slave(config)#
```

Related Commands

- [*nplus1 start master*](#) on page 247
- [*show nplus1*](#) on page 253

nplus1 stop

Stops N+1 slave or N+1 master controllers.

Syntax

nplus1 stop

Command Mode

Global Configuration

Default

NA

Usage

N+1 slave and N+1 master controllers must be stopped separately with the command **nplus1 stop**. Be sure to disable the master controller on the slave before stopping the master controller. Failure to disable the master will cause the slave to failover for the stopped master. Also, you can only issue **nplus1 stop** on a slave controller if the slave controller is not active (currently replacing a master controller).

Examples

This example stops N+1 on the slave controller named 3000-slave:

```
3000-slave(config)# nplus1 stop
```

Making this a normal controller.

This example stops N+1 on a master controller named 3000-1:

```
3000-1(config)# nplus1 stop
```

Related Commands

- [nplus1 start master on page 247](#)
- [nplus1 start slave on page 248](#)
- [show nplus1 on page 253](#)

nplus1 takeover

Manual failover from a master to a slave controller.

Syntax

nplus1 takeover

Command Mode

Global Configuration

Default

NA

Usage

Execute this command in the active master.

Examples

This example stops N+1 on the slave controller named 3000-slave:

```
3000-master(config)# nplus1 takeover
3000-master(config)#
```

Related Commands

- [*nplus1 start master on page 247*](#)
- [*nplus1 start slave on page 248*](#)
- [*show nplus1 on page 253*](#)

nplus1 timeout

The number of unreturned keepalives that trigger a standby slave to fail over.

Syntax

nplus1 timeout <number>

number The valid range is 4 to 60 (in seconds, one keepalive per second).

Command Mode

Global Configuration

Default

The default is 4.

Usage

The **nplus1 timeout** indicates the number of unreturned keep-alives that trigger a standby slave controller to take over for a master controller. When the indicated number is met, the standby controller becomes an active controller, takes over the IP address of the failed controller, and takes over for the unresponsive master.

Example

This example sets time-out to 60 seconds on the slave controller named 3000-slave:

```
3000-slave(config)# nplus1 timeout 60
```

Related Commands

- [nplus1 start master](#) on page 247
- [nplus1 start slave](#) on page 248

show nplus1

The **show nplus1** command checks the current controller configuration and shows the status of the controller.

Syntax

show nplus1

Command Mode

Privileged EXEC

Default

NA

Usage

Check that the software has started on either a master or slave controller with the **show nplus1** command. Also use the **show nplus1** command to verify that other commands have been executed. The descriptions of the display fields are provided in the following table:

Field	Description
Hostname	Hostname of the master controller
IP Address	Static IP address assigned to the master controller
Admin	Status of N+1 redundancy on the master: Enable—N+1 redundancy has been enabled on the master Disable—N+1 redundancy has been disabled
Switch	Ability of the slave to assume active slave for the master: Yes—Slave and master model/FortiWLC (SD) version number are compatible No—Slave and master model/FortiWLC (SD) version number are incompatible or the administrator has disabled N+1 on the master

Field	Description
Reason	<p>If Switch is No, describes why switch cannot be made:</p> <p>Down—Master has been disabled by the user</p> <p>SW Mismatch—The FortiWLC (SD) software is out of sync (update the master controller).</p> <p>No Access: the Passive Slave was not able to access the Master due to not receiving a copy of the configuration (a rare message that occurs if show nplus1 is executed almost immediately after adding a controller).</p> <p>No Access: the Passive Slave was not able to access the master controller (mostly occurs if a replacement controller has not had the access cleared using the nplus1 access command).</p> <p>WTR Set: As an Active Slave transitions back to Passive Slave this state is the first step in the WTR timer countdown.</p> <p>WTR <i>min</i>: After the WTR Set is reached, the timer counts down, showing the number of minutes (<i>min</i>) remaining.</p>
Adverts	Number of consecutively missed (not received) advertisements (a maximum of 5 triggers a failover if the Switch field is Yes).
SW Version	The software version of FortiWLC (SD) on the controller.

Examples

This example displays basic master controller identification information for the master named 3000-1:

```
NP-MC4200-master(15)# sh nplus1
-----
Master controller
Master IP : 172.19.215.31
Master Hostname : NP-MC4200-master
Master Status : Active
Slave IP : 172.19.215.32 <-- This is not displayed if Slave is not started
Slave Status : Passive <-- This is displayed as Unknown if slave is not started
-----
```

This example displays basic slave controller identification information on the slave controller named 3000-slave:

NP1-MC4200-slave(15)#sh nplus1

```

Current State : Passive
Heartbeat Period : 1000 milliseconds
Heartbeat Threshold : 4 threshold
Slave IP : 172.19.215.32
Slave Hostname : NP1-MC4200-slave
License Type : Demo
License Usage (Used/Tot) : 1/1
-----
Master Controllers
-----
Hostname      IP Address  Admin  Status Switch  Reason  MissedAdverts  SW Version
-----
MC4200-master 172.19.215.31  Enable  Active  Yes    -      0              6.1-2-15

```

This example displays information on an active slave—the master IP address and hostname are added to the display

```
NP-MC4200-master(15)# sh nplus1
-----
Current State : Active Slave
Heartbeat Period : 1000 milliseconds
Heartbeat Threshold : 4 threshold
Master IP : 172.19.215.31
Master Hostname : NP-MC4200-master
Slave IP : 172.19.215.32
Slave Hostname : NP1-MC4200-slave
License Type : Demo
License Usage (Used/Tot) : 1/1
-----
Master Controllers
-----

```

Hostname	IP Address	Admin	Status
NP-MC4200-master	172.19.215.31	Enable	Passive

**Related
Commands**

- [nplus1 add on page 238](#)
- [nplus1 add on page 238](#)
- [nplus1 delete on page 240](#)
- [nplus1 disable on page 241](#)
- [nplus1 revert on page 244](#)
- [nplus1 setdebugloglevel on page 246](#)
- [nplus1 start master on page 247](#)
- [nplus1 start slave on page 248](#)
- [nplus1 stop on page 250](#)

- *nplus1 timeout on page 252*

show nplus1 debugloglevel

Shows the level of verbosity set for the N+1 log messages.

Syntax `show nplus1 debugloglevel`

Command Mode Privileged EXEC

Default NA

Usage The `show nplus1 debugloglevel` command shows the level of verbosity set for the N+1 log messages.

Examples 3000-1# 3000-slave# `show nplus1 debugloglevel`
nplus1 Debug Logging Level: 0
3000-slave#

Related Commands [*nplus1 setdebugloglevel*](#) **on page 246**

7 Interface and IP Commands

The commands contained in this chapter are used to configure and show information about network interfaces:

- [*gw*](#) on page 261
- [*igmp-snoop*](#) on page 262
- [*interface FastEthernet*](#) on page 264
- [*ip address*](#) on page 266
- [*ip address dhcp*](#) on page 268
- [*ip default-gateway*](#) on page 269
- [*ip dhcp-passthrough*](#) on page 271
- [*ip dhcp-server*](#) on page 272
- [*ip dns-server*](#) on page 273
- [*ip domainname*](#) on page 274
- [*ip ftp*](#) on page 275
- [*ip scp*](#) on page 276
- [*ip sftp*](#) on page 277
- [*ip udp-broadcast*](#) on page 278
- [*ipv6-neighbor-discovery-optimization*](#) on page 280
- [*mac-address*](#) on page 281
- [*port-profile*](#) on page 282
- [*\(config-port-profile\) ap-vlan-tag*](#) on page 283
- [*\(config-port-profile\) dataplane*](#) on page 284
- [*\(config-port-profile\) disable*](#) on page 285
- [*\(config-port-profile\) enable*](#) on page 286
- [*\(config-port-profile\) multicast-enable*](#) on page 287
- [*\(config-port-profile\) show*](#) on page 288
- [*\(config-port-profile\) vlan*](#) on page 289
- [*show igmp-snoop*](#) on page 292

- [show interfaces FastEthernet ap](#) on page 294
- [show interfaces FastEthernet controller](#) on page 297
- [show interfaces FastEthernet statistics](#) on page 300
- [show ip](#) on page 302
- [show ipv6-neighbor](#) on page 304
- [show second_interface_status](#) on page 305
- [static-route](#) on page 306
- [\(config-static-route\) interface](#) on page 307
- [\(config-static-route\) ip](#) on page 308
- [type](#) on page 309
- [virtual-interface-profile](#) on page 311
- [\(config-vip\) disable](#) on page 312
- [\(config-vip\) enable](#) on page 313
- [\(config-vip\) gateway](#) on page 314
- [\(config-vip\) ip](#) on page 315
- [\(config-vip\) show](#) on page 316

gw

Configures the FastEthernet interface gateway IP address.

Syntax

gw <address>

address Sets the IP address for the gateway.

Command Mode

FastEthernet interface configuration mode

Default

NA

Usage

This command configures the gateway IP address that is used by the FastEthernet interface. The **gw** configuration is a mandatory field when the interface is configured for active operation (that is, the FastEthernet interface **type** is configured as **active**).

Examples

The following commands configure Ethernet port 2 as an **active** interface that can be used to support a VLAN or GRE (Generic Routing Encapsulation) tunneling. The **ip address** specifies the IP address of interface followed by the associated netmask. The **gw** command specifies the gateway configuration, and is a mandatory field.

```
default# configure terminal
default(config)# interface FastEthernet 2
default(config-if-FastEth)# ip address 172.26.16.200 255.0.0.0
default(config-if-FastEth)# gw 172.26.16.1
default(config-if-FastEth)# type active
default(config-if-FastEth)# end
```

Related Commands

- [ip address on page 266](#)
- [show interfaces FastEthernet controller on page 297](#)
- [show second_interface_status on page 305](#)
- [type on page 309](#)

igmp-snoop

Configures IGMP snooping.

Syntax

```
igmp-snoop enable
iiigmp-snoop age-time <duration>
iiigmp-snoop disable
```

duration	Sets the number of seconds before a timeout is implemented for an IGMP group. <i>duration</i> can be between 1 and 300 seconds Multicast subscriptions from the client are aged out when there are no reports from the last IGMP report before the age timeout interval. For every IGMP report for the multicast group the IGMP daemon resets the age timeout (the timeout when a group entry has to be deleted if there is no explicit leave for the group from a client) for the multicast group on an ESS for a particular client.
----------	--

Command Mode

Global configuration mode

Limitations

This feature is not supported for dynamic VLANs. This feature is not supported for non-IPv4 multicast.

Default

IGMP snooping is disabled.

Usage

IGMP Snooping helps an L2 device make intelligent multicast forwarding decisions by sniffing for the IGMP protocol messages and building a multicast forwarding table; hence, it can significantly reduce traffic from streaming media and other bandwidth-intensive IP multicast applications. IGMP versions v1 through v3 are supported.

If this feature is disabled, when the controller receives southbound IP multicast traffic, it forwards the IP multicast packet to every associated AP. This can result in excessive traffic to APs whose clients have not subscribed to IP multicast traffic.

By default, an L2 Switch/Bridge treats IP multicast traffic in the same manner as broadcast traffic by forwarding frames received on one interface to all other interfaces. This may create excessive traffic on the network and degrade the performance of hosts attached to the network.

The IGMP protocol is used by stations to subscribe and unsubscribe to an IP multicast group (address). A station that wishes to join a particular IP multicast group sends a “group join” message to the L3 device so that the L3 device records the IP multicast group address and the interface in its routing table. The L3 device forwards the traffic to the IP multicast address only to the interfaces from which it has received join messages.

The L3 device periodically send queries to find out if the stations are still interested in receiving the IP multicast traffic to a particular group. The interested stations respond to the IGMP query. Based on the response from the stations, the L3 device prunes the routing table.

IGMP v2 and v3 provide a mechanism to the stations to send explicit “group leave” message to the L3 device so that the stations can unsubscribe to the particular IP multicast group.

These IGMP protocol messages pass through the L2 device between the L3 device and the station. The controller acts as a L2 device in the network. IGMP Snooping in the controller applies only tunneled multicast traffic.

When the controller receives a southbound IP multicast traffic, it forwards the IP multicast packet to every associated AP. This brings in excessive traffic to APs whose clients have not subscribed to IP multicast traffic. This warrants a need for IGMP Snooping feature in controller.

Examples

The following commands enable IGMP snooping and set the ageout to 240 seconds.

```
controller(config)# igmp-snoop enable
controller(config-if-FastEth)# igmp-snoop age-time 240
```

Related Commands

[*show igmp-snoop*](#) on [*page 292*](#)

interface FastEthernet

Configures the controller FastEthernet interface.

Syntax

interface FastEthernet <interface_index>

interface_index Selects the interface port for configuration, either **1** or **2**.

Command Mode

Global configuration

Default

NA

Usage

This command selects the FastEthernet interface to be configured and enters the FastEthernet configuration submode.

The controller has two FastEthernet interfaces: the first is configured when the controller is first set up using the **setup** command. Subsequent modifications to that interface, and configuration for the second interface are performed with this command. The following shows the command to edit interface 1 and the commands that are available from within the FastEthernet configuration submode:

```
default(config)# interface FastEthernet 1
default(config-if-FastEth)# ?
do                               Executes an IOSCLI command.
end                               Save changes, and return to privileged EXEC mode.
exit                             Save changes, and return to global configuration
mode.
gw                               Configure Gateway IP Address.
ip                               Configure IP Address and Netmask.
type                             Configure the type of the interface.
```

The submode commands include the **ip address** command to set the IP address for the interface (also referred as the local endpoint for VLAN and GRE tunnel configurations). The address can be set to a static IP address (**ip address nnn.nnn.nnn.nnn**) or through DHCP (**ip address dhcp**).

The **gw** command sets the default gateway IP address used by the interface.

The **type** command determines how the interface is used: as a **redundant** port to interface 1 or as a second fully-functional **active** port.

Example

The following commands configure Ethernet interface 2 as a backup to Ethernet interface 1, as specified by **redundant** for the **type** option. No IP address should be assigned when the type is redundant.

```
default# configure terminal
default(config)# interface FastEthernet 2
default(config-if-FastEth)# type redundant
default(config-if-FastEth)# end
```

The following commands configure Ethernet port 2 as an **active** interface that can be used to support a VLAN or GRE (Generic Routing Encapsulation) tunneling. The **ip address** specifies the IP address of the VLAN or GRE local endpoint followed by the associated net-mask. The **gw** command specifies the gateway configuration, and is a mandatory field. The gateway is the IP address of the VLAN or GRE tunnel remote endpoint.

```
default# configure terminal
default(config)# interface FastEthernet 2
default(config-if-FastEth)# ip address 172.26.16.200 255.0.0.0
default(config-if-FastEth)# gw 172.26.16.1
default(config-if-FastEth)# type active
default(config-if-FastEth)# end
```



In the active configuration, the second Ethernet interface must be configured with a static IP address (not DHCP) to a different L2 domain as the primary interface.



The port bonding mode must be set to dual or none (depending on the controller model) before configuring the second interface for redundant or active mode. To configure bonding, refer to the FortiWLC (SD) Configuration Guide.

Related Commands

- [gw on page 261](#)
- [ip address on page 266](#)
- [show interfaces FastEthernet controller on page 297](#)
- [show second_interface_status on page 305](#)
- [type on page 309](#)

ip address

Configures static IP address connectivity.

Syntax

ip address <ip-address> <ip-netmask>

ip-address Sets the IP address for *address*.

ip-netmask Sets the IP address netmask to *netmask*

Command Mode

Global, FastEthernet, RADIUS Profile, AP connectivity, and VLAN configuration modes

Default

NA

Usage

Note that this command cannot be executed in config mode; the user must execute it from FastEthernet, AP, or VLAN configuration mode. This command configures the IP address and netmask for a controller, RADIUS server, access point, or VLAN, depending on the submode in which this command is invoked.

When configuring the IP address of the AP, the AP is a Remote AP and you are configuring a static IP address. You can also configure the AP to use a dynamic IP address with the **ip address dhcp** command.

When configuring the IP address in the VLAN submode, the IP address specified for the VLAN must match the default gateway configured in the client.

Examples

To assign a static IP address to the controller, use the **ip address** command with the IP address and subnet arguments, as follows:

```
controller(config-ap)# ip address 10.0.0.19 255.0.0.0
```

To assign a static IP address to the Remote AP, enter the AP connectivity submode. Then use the **ip address** command to configure the IP address 10.0.220.30 and netmask 255.255.255.0 for the Remote AP.

```
controller(config)# ap 1
controller(config-ap)# 13-connectivity 13-preferred
controller(config-ap-connectivity)# ip address 10.0.220.30 255.255.255.0
```

```
controller(config-ap-connectivity)#
```

The following command specifies the IP address 10.1.2.3 and netmask 255.0.0.0 for a VLAN.

```
controller(config)# vlan qa tag 100
```

```
controller(config-vlan)# ip address 10.1.2.3 255.0.0.0
```

Related Commands

- [gw](#) on page 261
- [interface FastEthernet](#) on page 264
- [ip address dhcp](#) on page 268
- [ip default-gateway](#) on page 269
- [ip dns-server](#) on page 273
- [show ap-connectivity](#) on page 630
- [show controller](#) on page 173
- [type](#) on page 309

ip address dhcp

Configures DHCP connectivity.

Syntax

ip address dhcp

Command Mode

Global and AP connectivity configuration modes

Default

NA

Usage

Note that this command cannot be executed in config mode; the user must execute it from FastEthernet, AP, or VLAN configuration mode. This command configures DHCP connectivity for a controller and access point, depending on the submode in which this command is invoked.

Examples

To allow the controller to be assigned a dynamic IP address, use the **ip address dhcp** command, as follows:

```
controller(config-ap)# ip address dhcp
```

To allow the AP to be assigned a dynamic IP address, enter the AP connectivity submode. Then use the **ip address dhcp** command to configure a dynamically assigned IP address for the Remote AP.

```
controller(config)# ap 1
controller(config-ap)# 13-connectivity 13-preferred
controller(config-ap-connectivity)# ip address dhcp
controller(config-ap-connectivity)#
```

Related Commands

- [ip default-gateway on page 269](#)
- [ip dns-server on page 273](#)
- [show controller on page 173](#)

ip default-gateway

Configures default gateway connectivity.

Syntax

ip default-gateway <address>

address IP address of the default gateway.

Command Mode

Global configuration, AP connectivity configuration, and VLAN configuration modes

Default

The default IP address of the default gateway is 0.0.0.0.

Usage

Note that this command cannot be executed in config mode; the user must execute it from FastEthernet, AP, or VLAN configuration mode. Configures default gateway connectivity for the controller, access point, or VLAN, depending on the submode under which the command is invoked.

When configuring the default gateway for a VLAN, use the default gateway used by the controller to route traffic coming from wireless clients using the VLAN.

Use the **default** form to set the default gateway to its default value.

Examples

To assign the default gateway IP address used by the controller, use the **ip default-gateway** command with the IP address, as follows:

```
controller(config-ap)# ip default-gateway 10.0.0.1
```

To assign the default gateway IP address used by the AP, enter the AP connectivity submode. Then use the **ip default-gateway** command to configure the IP address for the Remote AP.

```
controller(config)# ap 1
controller(config-ap)# 13-connectivity 13-preferred
controller(config-ap-connectivity)# ip default-gateway 10.0.0.1
```

To assign the default gateway IP address used by the VLAN, for example:

```
controller(config)# vlan qa tag 100
```

```
controller(config-vlan)# ip default-gateway 10.0.0.1
```

Related Commands

- [ip address](#) on page 266
- [ip address dhcp](#) on page 268
- [ip dns-server](#) on page 273
- [show ap-connectivity](#) on page 630
- [show controller](#) on page 173

ip dhcp-passthrough

Enables or disables the DHCP pass-through.

Syntax

```
ip dhcp-passthrough
no dhcp-passthrough
```

Command Mode

Global configuration and VLAN configuration modes

Default

DHCP pass-through is enabled.

Usage

This command enables or disables (using the **no** form) the DHCP pass-through service for the controller or the VLAN, depending on the submode under which the command is invoked. If enabled, and if the DHCP server IP is the default 127.0.0.1, DHCP packets pass through without modification (as in a bridge). The pass-through behavior eliminates the need for the DHCP relay in most installations, and puts the burden of relay on the routers, which is traditional.

Global DHCP passthrough is overridden by a corresponding module's DHCP pass-through configuration.

Examples

To enable DHCP pass-through for the controller, use the **ip dhcp-passthrough** command, as follows:

```
controller(config)# ip dhcp-passthrough
```

To enable DHCP pass-through for the VLAN, for example:

```
controller(config)# vlan qa tag 100
controller(config-vlan)# ip dhcp-passthrough
```

Related Commands

- [ip dhcp-server on page 272](#)
- [show controller on page 173](#)

ip dhcp-server

Configures the DHCP relay server.

Syntax

```
ip dhcp-server <ip-address>  
no ip dhcp-server
```

ip-address IP address of the DHCP relay server in dotted decimal notation (*n.n.n.n*).

Command Mode

Global configuration and VLAN configuration modes

Default

The default IP address of the DHCP relay server is 127.0.0.1.

Usage

This command configures the DHCP relay server for the controller and VLAN, depending on the submode under which the command is invoked.

If specified in VLAN submode, the specified DHCP server overrides the controller-assigned DHCP server configuration. Because of some interoperability configurations, FortiWLC (SD) also supports the use of the IP address 255.255.255.255 as a valid DHCP relay address.

Use the **no** form to remove the DHCP relay server.

Examples

To configure a DHCP relay server for the controller, use the **ip dhcp-server** command, as follows:

```
controller(config)# ip dhcp-server 10.0.1.20
```

To configure a DHCP server for the VLAN, for example:

```
controller(config)# vlan qa tag 100  
controller(config-vlan)# ip dhcp-server 10.0.0.1
```

Related Commands

- [ip dhcp-passthrough on page 271](#)
- [show controller on page 173](#)

ip dns-server

Configures a DNS server's IP address.

Syntax

```
ip dns-server <ip_addr>
ip dns-server primary <ip_addr>    (for AP connectivity sub-mode only)
ip dns-server secondary} <ip_addr>  (for AP connectivity sub-mode only)
no ip dns-server
```

ip_addr IP address of the DNS server in dotted decimal notation (*n.n.n.n*).

Command Mode

Global configuration and AP connectivity configuration modes

Default

By default, no DNS server is configured.

Usage

Use this command to add a DNS server by specifying its IP address. After the DNS servers have been added, when needed, the system will connect to the first DNS server if it is able to; otherwise, it will go on to the next one until it finds one that is working.

Use the **no** form to remove the DNS server.

Examples

To assign a DNS server IP address used by the controller, use the **ip dns-server** command with the IP address, as follows:

```
controller(config)# ip dns-server 10.0.200.1
```

To assign a DNS server IP address used by the AP, enter the AP connectivity submode. Then use the **ip dns-server primary** or **ip dns-server secondary** command to configure the DNS server IP address used by the Remote AP:

```
controller(config)# ap 1
controller(config-ap)# 13-connectivity 13-preferred
controller(config-ap-connectivity)# ip dns-server primary 10.0.0.1
```

Related Commands

- [ip address on page 266](#)
- [ip address dhcp on page 268](#)
- [ip default-gateway on page 269](#)

ip domainname

Configures the DNS domain name.

Syntax

```
ip domainname <name>  
no ip domainname
```

name Specifies the domain using from 1 to 63 characters.

Command Mode

Global configuration

Default

NA

Usage

Sets the domain name for use with DNS. Use the **no** command form to remove the configured domain name.

Examples

To assign a domain name for use by DNS, type **configure terminal** to enter global configuration mode, and use the **ip domainname** command with the name, as follows:

```
controller(config)# ip domainname fortinet.com
```

Related Commands

- [ip address on page 266](#)
- [ip address dhcp on page 268](#)
- [ip default-gateway on page 269](#)
- [ip dns-server on page 273](#)

ip ftp

Configures a username/password for FTP.

Syntax

```
ip ftp username <username>  
ip ftp password <username> <password>
```

<i>username</i>	Specifies the FTP username.
<i>password</i>	Specifies the FTP password.

Command Mode

Global configuration

Default

NA

Usage

Sets the default username and password for an FTP session.

Examples

To set the FTP username to susanne for the session:

```
controller(config)# ip ftp username susanne
```

Related Commands

- [ip address](#) on page 266
- [ip address dhcp](#) on page 268
- [ip default-gateway](#) on page 269
- [ip dns-server](#) on page 273

ip scp

Configures the username/password for SCP.

Syntax

```
ip scp username <username>  
ip scp password <username> <password>
```

<i>username</i>	Specifies the SCP username. The name can be a maximum of 32 characters.
<i>password</i>	Specifies the SCP password. The password can be a maximum of 32 characters.

Command Mode

Global configuration

Default

Usage

Sets the default username and password for an SCP session.

Examples

To set the SFTP username to suzanne for the session:

```
controller(config)# ip scp username suzanne
```

Related Commands

- [ip address](#) on page 266
- [ip address dhcp](#) on page 268
- [ip default-gateway](#) on page 269
- [ip dns-server](#) on page 273

ip sftp

Configures the username/password for SFTP.

Syntax

```
ip sftp username <username>  
ip sftp password <username> <password>
```

<i>username</i>	Specifies the SFTP username.
<i>password</i>	Specifies the SFTP password.

Command Mode

Global configuration

Default

NA

Usage

Sets the default username and password for an SFTP session.

Examples

To set the SFTP username to suzann for the session:

```
controller(config)# ip sftp username suzann
```

Related Commands

- [ip address](#) on page 266
- [ip address dhcp](#) on page 268
- [ip default-gateway](#) on page 269
- [ip dns-server](#) on page 273

ip udp-broadcast

Configures UDP broadcast ports.

Syntax

```
ip udp-broadcast upstream <port_number>
ip udp-broadcast upstream-bridged <port_number>
ip udp-broadcast downstream <port_number>
ip udp-broadcast downstream-bridged <port_number>
no ip udp-broadcast upstream <port_number>
no ip udp-broadcast upstream-bridged <port_number>
no ip udp-broadcast downstream <port_number>
no ip udp-broadcast downstream-bridged <port_number>
```

port_number Specifies the upstream or downstream port number (1 to 65535).

Command Mode

Global configuration

Default

No ports are configured.

Usage

This command is required if you are going to pass broadcast traffic for an application. It configures the set of UDP ports inspected for a broadcast destination address and sent either upstream as broadcast on the wired interface or downstream onto the wireless interfaces. The maximum number of ports that can be configured is 8 per direction. Use the **no** form to remove the udp broadcast port. This feature also configures udp broadcast support between wireless stations.

Examples

To configure Wireless to Wireless UDP broadcast, enable upstream and downstream broadcast for the port. In this example, the feature is enabled for port 10000 by the following CLI commands:

```
configure terminal
ip udp-broadcast upstream 10000
ip udp-broadcast downstream 10000
end
```

To configure port 5455 to be used as a UDP broadcast to wireless clients for example, use the following command:

```
controller(config)# ip udp-broadcast downstream 5455
```

To cancel the configured upstream port number 3822 for example, use the following command:

```
controller(config)# no ip udp-broadcast upstream 3822
```

Related Commands

- [ip address](#) on page 266
- [ip address dhcp](#) on page 268
- [ip default-gateway](#) on page 269
- [ip dns-server](#) on page 273

ipv6-neighbor-discovery-optimization

Enable or disable the IPV6 neighbor discovery optimization feature.

Syntax

`ipv6-neighbor-discovery-optimization`

Command Mode

Global configuration

Default

None

Usage

Use this command to enable or disable the ipv6 neighbor discovery optimization feature.

Examples

```
MC3200(15)# configure terminal
MC3200(15)(config)# ipv6-neighbor-discovery-optimization enable
MC3200(15)(config)#
```

Related Commands

[*show ipv6-neighbor*](#) on page 304

mac-address

Configures the MAC address of the Ethernet interface.

Syntax

mac-address <MAC-address>

mac-address MAC address of the Ethernet interface, specified in hexadecimal format (xx:xx:xx:xx:xx:xx:xx:xx).

Command Mode

Interface Configuration

Default

None

Usage

Enter the MAC address to configure the Ethernet interface.

Examples

```
mc1100# (config)# ap 1
mc1100# (config-ap)# mac-address 00:12:F2:00:00:59
mc1100# (config-ap)#
```

Related Commands

[show interfaces FastEthernet ap](#) on page 294

port-profile

Allows you to create and configure a Port Profile.

Syntax

port-profile <*profile*>

profile The name of the profile to be modified or created.

Command Mode

Global configuration

Default

NA

Usage

This command is used to access port profile properties and make changes by using the other commands documented in this chapter. All port profile-based commands are performed while in port profile configuration mode.

Examples

```
default(15)# configure terminal
default(15)(config)# port-profile port1
default(15)(config-port-profile)#
```

Related Commands

- [\(config-port-profile\) ap-vlan-tag on page 283](#)
- [\(config-port-profile\) dataplane on page 284](#)
- [\(config-port-profile\) disable on page 285](#)
- [\(config-port-profile\) enable on page 286](#)
- [\(config-port-profile\) multicast-enable on page 287](#)
- [\(config-port-profile\) show on page 288](#)
- [\(config-port-profile\) vlan on page 289](#)

(config-port-profile) ap-vlan-tag

Allows you to specify the VLAN tag for the current port profile.

Syntax

ap-vlan-tag <VLAN>

VLAN The VLAN tag to be assigned to the port profile. This can range from 1 to 4094.

Command Mode

Port Profile configuration

Default

NA

Usage

This command is used to specify the VLAN tag to be used for the current port profile. The VLAN tag is used only when operating in bridged mode.

Examples

```
default(15)# configure terminal
default(15)(config)# port-profile port1
default(15)(config-port-profile)# ap-vlan-tag 14
default(15)(config-port-profile)#
```

Related Commands

- [port-profile on page 282](#)
- [\(config-port-profile\) dataplane on page 284](#)
- [\(config-port-profile\) disable on page 285](#)
- [\(config-port-profile\) enable on page 286](#)
- [\(config-port-profile\) multicast-enable on page 287](#)
- [\(config-port-profile\) show on page 288](#)
- [\(config-port-profile\) vlan on page 289](#)

(config-port-profile) dataplane

Allows you to switch the port profile between bridged and tunneled modes.

Syntax

dataplane <mode>

mode Specify *bridged* or *tunneled* as desired.

Command Mode

Port Profile configuration

Default

Tunneled

Usage

This command is used to specify whether the port profile should be used for bridged or tunneled operation.

Examples

```
default(15)# configure terminal
default(15)(config)# port-profile port1
default(15)(config-port-profile)# dataplane bridged
default(15)(config-port-profile)#
```

Related Commands

- [port-profile](#) on page 282
- [\(config-port-profile\) ap-vlan-tag](#) on page 283
- [\(config-port-profile\) disable](#) on page 285
- [\(config-port-profile\) enable](#) on page 286
- [\(config-port-profile\) multicast-enable](#) on page 287
- [\(config-port-profile\) show](#) on page 288
- [\(config-port-profile\) vlan](#) on page 289

(config-port-profile) disable

Disables the current Port Profile.

Syntax **disable**

Command Mode Port Profile configuration

Default Disabled

Usage This command is used to disable the active Port Profile.

Examples

```
default(15)# configure terminal
default(15)(config)# port-profile port1
default(15)(config-port-profile)# disable
default(15)(config-port-profile)#
```

Related Commands

- [port-profile on page 282](#)
- [\(config-port-profile\) ap-vlan-tag on page 283](#)
- [\(config-port-profile\) dataplane on page 284](#)
- [\(config-port-profile\) enable on page 286](#)
- [\(config-port-profile\) multicast-enable on page 287](#)
- [\(config-port-profile\) show on page 288](#)
- [\(config-port-profile\) vlan on page 289](#)

(config-port-profile) enable

Enables the current Port Profile.

Syntax

enable

Command Mode

Port Profile configuration

Default

Disabled

Usage

This command is used to enable the active Port Profile.

Examples

```
default(15)# configure terminal
default(15)(config)# port-profile port1
default(15)(config-port-profile)# enable
default(15)(config-port-profile)#
```

Related Commands

- [port-profile on page 282](#)
- [\(config-port-profile\) ap-vlan-tag on page 283](#)
- [\(config-port-profile\) dataplane on page 284](#)
- [\(config-port-profile\) disable on page 285](#)
- [\(config-port-profile\) multicast-enable on page 287](#)
- [\(config-port-profile\) show on page 288](#)
- [\(config-port-profile\) vlan on page 289](#)

(config-port-profile) multicast-enable

Enables the transmission of multicast frames to and from this port profile.

Syntax

```
multicast-enable
no multicast-enable
```

Command Mode

Port Profile configuration

Default

Off

Usage

This command is used to configure the Allow Multicast flag in the port profile. To enable multicast transmissions on this port, simply enter the **multicast-enable** command. To disable them, enter **no multicast-enable**. The example below enables and then disables multicast on the port1 profile.

Examples

```
default(15)# configure terminal
default(15)(config)# port-profile port1
default(15)(config-port-profile)# multicast-enable
default(15)(config-port-profile)#
default(15)(config-port-profile)# multicast-disable
default(15)(config-port-profile)#
```

Related Commands

- [port-profile on page 282](#)
- [\(config-port-profile\) ap-vlan-tag on page 283](#)
- [\(config-port-profile\) dataplane on page 284](#)
- [\(config-port-profile\) disable on page 285](#)
- [\(config-port-profile\) enable on page 286](#)
- [\(config-port-profile\) show on page 288](#)
- [\(config-port-profile\) vlan on page 289](#)

(config-port-profile) show

Allows you to display the current Port Profile being modified.

Syntax

show context

Command Mode

Port Profile configuration

Default

NA

Usage

This command is used to view the active Port Profile.

Examples

```
default(15)# configure terminal
default(15)(config)# port-profile port1
default(15)(config-port-profile)# show context
Port Profile Name: port1
default(15)(config-port-profile)#
```

Related Commands

- [port-profile on page 282](#)
- [\(config-port-profile\) ap-vlan-tag on page 283](#)
- [\(config-port-profile\) dataplane on page 284](#)
- [\(config-port-profile\) disable on page 285](#)
- [\(config-port-profile\) enable on page 286](#)
- [\(config-port-profile\) multicast-enable on page 287](#)
- [\(config-port-profile\) vlan on page 289](#)

(config-port-profile) vlan

Specifies the name for the VLAN to be accessed by the port profile.

Syntax

vlan <name>

name The name of the VLAN.

Command Mode

Port Profile configuration

Default

NA

Usage

This command is used to configure the name of the VLAN serviced by the configured port.

Examples

```
default(15)# configure terminal
default(15)(config)# port-profile port1
default(15)(config-port-profile)# vlan v1
default(15)(config-port-profile)#
```

Related Commands

- [port-profile on page 282](#)
- [\(config-port-profile\) ap-vlan-tag on page 283](#)
- [\(config-port-profile\) dataplane on page 284](#)
- [\(config-port-profile\) disable on page 285](#)
- [\(config-port-profile\) enable on page 286](#)
- [\(config-port-profile\) multicast-enable on page 287](#)
- [\(config-port-profile\) show on page 288](#)

(config-port-profile) ip-prefix-validation-enable

In a situation where a station with an IP address from a different subnet connects to the controller, it can result in various network issues including outage. Enabling IP prefix validation prevents stations with different subnet connecting to the controller. By default, IP Prefix Validation in Port Profile it is OFF.

Syntax

ip-prefix-validation-enable

name The name of the VLAN.

Command Mode

Port Profile configuration

Default

NA

Usage

This command is used to enable or disable IP Prefix validation.

Examples

```
default(15)# configure terminal
default(15)(config)# port-profile port1
default(15)(config-port-profile)# ip-prefix-validation-enable
default(15)(config-port-profile)#
```

Related Commands

- [port-profile on page 282](#)
- [\(config-port-profile\) ap-vlan-tag on page 283](#)
- [\(config-port-profile\) dataplane on page 284](#)
- [\(config-port-profile\) disable on page 285](#)
- [\(config-port-profile\) enable on page 286](#)
- [\(config-port-profile\) multicast-enable on page 287](#)

(config-port-profile) show on page 288

show igmp-snoop

Displays information related to the state of IGMP snooping.

Syntax

```
show igmp-snoop forwarding-table  
show igmp-snoop subscription-table]
```

Command Mode

Privileged EXEC mode

Default

NA

Usage

This command displays whether IGMP snooping is enabled or disabled, and if enabled, the number of seconds before the device ages out of the IGMP snoop group.

With the optional argument **forwarding-table**, the list of participating ESS IDs, MAC address of the APs, Mutlicast group name, and filtering mode information is produced.

With the optional argument **subscription-table**, the list of participating ESS IDs, MAC address of the APs, MAC address of subscribing clients, and Multicast information is produced.

Examples

```
controller# show igmp-snoop  
IGMP Snoop
```

```
IGMP Snoop Enable/Disable      : enable  
IGMP Snoop expiration timer period : 240
```

```
MC500# show igmp-snoop forwarding-table
```

Ess ID	AP MAC	Multicast Group	Filter Mode	Source List
--------	--------	-----------------	-------------	-------------

```
IGMP Snoop forward table(No entries)
```

```
MC500# show igmp-snoop subscription-table  
<CR>
```


MC500# show igmp-snoop subscription-table

Ess ID	AP MAC	Client MAC	Multicast Group
Aging Time	Filter Mode	Source List	

IGMP Snoop subscription table (No entries)

**Related
Commands**

[igmp-snoop](#) *on page 262*

show interfaces FastEthernet ap

Displays information related to the FastEthernet configuration for an access point.

Syntax

`show interfaces FastEthernet ap [ap-id] [interface index]`

- ap-id

Specifies a unique identifier for the access point.
- interface index

Specifies the interface to be displayed. Since some AP models have multiple interfaces, the user must specify the desired option.

Command Mode

Privileged EXEC mode

Default

NA

Usage

This command displays FastEthernet Interface configuration information for all APs, or the specified access point. The following information is provided:

Parameter	Description
Type	The type of node, for example, access point.
ID	The unique identifier for the access point.
Name	The access point name.
Interface Index	The index for identifying this interface.
MTU	The Maximum Transmission Unit (MTU) for the interface.
MAC Address	The MAC address of the interface.
Admin State	The administrative state of the interface, the state can be Up or Down .
Operational State	The status of the interface. Status can be Enabled or Disabled .

Parameter	Description
Last Changed	The date the interface was changed last.
Uplink Type	Displays whether the interface is set for uplink or downlink connectivity.

Examples

The following command displays FastEthernet configuration for all APs:

```
controller# show interfaces FastEthernet ap
Type ID Name IfIndex MTU MAC Address Admin State Op State Last Change
Uplink Type
ap 170 AP-170 2 1500 00:0c:e6:0d:ef:87 Up Disabled 06/06/2013 09:09:34
Downlink
ap 170 AP-170 1 1500 00:0c:e6:0d:ef:87 Up Disabled 06/06/2013 09:09:34
Uplink
ap 169 AP-169 2 1500 00:0c:e6:0d:ef:71 Up Disabled 06/06/2013 09:09:34
Downlink
ap 169 AP-169 1 1500 00:0c:e6:0d:ef:71 Up Disabled 06/06/2013 09:09:34
Uplink
ap 167 AP-167 2 1500 00:0c:e6:0d:ee:aa Up Disabled 06/06/2013 09:09:34
Downlink
ap 167 AP-167 1 1500 00:0c:e6:0d:ee:a9 Up Enabled 06/06/2013 09:11:29
Uplink Interface Table(6)
```

The following command displays FastEthernet configuration information for AP 1:

```
controller# show interfaces FastEthernet ap 167
Type ID Name IfIndex MTU MAC Address Admin State Op State Last Change
Uplink Type
ap 167 AP-167 1 1500 00:0c:e6:0d:ee:a9 Up Enabled 06/06/2013 09:11:29
Uplink
ap 167 AP-167 2 1500 00:0c:e6:0d:ee:aa Up Disabled 06/06/2013 09:09:34
Downlink
Ethernet Table(2 entries)
```

The following command displays FastEthernet configuration information for a particular interface on the AP:

```
controller# show interfaces FastEthernet ap 167 1
Ethernet Table
Node Type : ap
```

Node ID : 167
Node Name : AP-167
Interface Index : 1
Description : eth0-167-1
MTU : 1500
Interface Speed (Mbits/sec) : 1000
Duplex Mode : full-duplex
Physical Address : 00:0c:e6:0d:ee:a9
Administrative State : Up
Operational State : Enabled
Last Changed : 06/06/2013 09:11:29
Uplink Type : Uplink

Related Commands

[interface FastEthernet](#) on page 264

show interfaces FastEthernet controller

Displays information related to the FastEthernet configuration for the controller.

Syntax `show interfaces FastEthernet controller`

Command Mode Privileged EXEC mode

Default NA

Usage This command displays FastEthernet Interface configuration information for the controller. The following information is provided:

Parameter	Description
Node Type	The type of node, for example, controller.
Node ID	The unique identifier for the controller.
Node Name	The name assigned to the controller.
Interface Index	The index for identifying this interface.
Description	Shows a description of the interface.
MTU	The Maximum Transmission Unit (MTU) for the interface.
Interface Speed (Mbits/sec)	The configured speed for the interface.
Duplex Mode	Indicates whether the interface is using full-duplex or half-duplex mode.
Physical MAC Address	The MAC address of the interface.
Operational State	The status of the interface. Status can be Enabled or Disabled .
Last Changed	The date the interface was changed last.
In Octets	The number of octets received by this interface.

Parameter	Description
In Unicast Packets	The number of unicast packets received by this interface.
In Non-Unicast Packets	The number of non-unicast packets received by this interface.
In Discards	The number of incoming packets discarded by this interface.
In Errors	The number of incoming packets with errors on this interface.
In Unknown Protocols	The number of packets with an unknown protocol received by this interface.
Out Octets	The number of octets sent by this interface.
Out Unicast Packets	The number of unicast packets sent by this interface.
Out Non-Unicast Packets	The number of non-unicast packets sent by this interface.
Out Discards	The number of outgoing packets discarded by this interface.
Out Errors	The number of outgoing packets with errors on this interface.
Out Queue Length	The number of packets in the outgoing packet queue.

Examples

The following command displays FastEthernet configuration information for the controller:

```

controller# show interfaces FastEthernet controller
Type          ID  Name          MTU      MAC Address      Op State  Last
Change
controller 1  controller    1500     00:90:0b:07:d0:82 Enabled    2008/
03/07 09:22:26

      Interface Table(1 entry)
Interface Table
Node Type          : controller
Node ID            : 1
Node Name          : controller1
Interface Index     : 3
Description        : eth1
MTU                : 1500
Interface Speed (Mbits/sec) : 100
Duplex Mode        : full-duplex
Physical Address    : 00:02:b3:e6:d7:12

```

Operational State	: Enabled
Last Changed	: -
Description	: eth1
In Octets	: 272189914
In Unicast Packets	: 1638979
In Non-Unicast Packets	: 0
In Discards	: 0
In Errors	: 0
In Unknown Protocols	: 0
Out Octets	: 1467641108
Out Unicast Packets	: 9827811
Out Non-Unicast Packets	: 0
Out Discards	: 0
Out Errors	: 0

Related Commands

[interface FastEthernet](#) on page 264

show interfaces FastEthernet statistics

Displays statistics related to the FastEthernet interface.

Syntax `show interfaces FastEthernet statistics ap <ap_id>
show interfaces FastEthernet statistics controller]`

Command Mode Privileged EXEC mode

Default NA

Usage This command displays statistics for the FastEthernet AP or controller interface. The following information is provided:

Statistic	Description
IfIndex	The index for identifying the interface.
Node ID	The unique identifier for the node (controller or AP).
Node Name	The name assigned to the node.
Type	The type of node, for example, controller or AP.
In Octets	The number of octets received by this interface.
In Errors	The number of errors received by this interface.
Out Octets	The number of octets sent by this interface.
Out Errors	The number of errors sent by this interface.

Examples The following command displays FastEthernet statistics for the controller and associated APs:

```
controller# show interfaces FastEthernet statistics  
Ethernet Statistics
```


IfIndex	Node ID	Node Name	Type	In Octets	In Errors	Out
Octets	Out	Errors				
2	1	forti-wifi	controller	566589467	0	
192971219		0				
100	2	#2-2F-Sw-208	ap	665578131	0	
328290792		0				
100	3	#3-2F-Exec-201	ap	124603915	0	
84559243		0				
100	11	AP-11	ap	123112809	0	
545091756		0				
100	12	AP-12	ap	0	0	
0						

Ethernet Statistics(5 entries)

show ip

Displays IP configuration information.

Syntax

```
show ip
show ip default-gateway
show ip dhcp-server
show ip dns-server
show ip domainname
```

Command Mode

Privileged EXEC mode

Default

Shows IP address information for the controller.

Usage

Use this command to obtain IP addresses assigned to the controller, default gateway, DHCP and DNS servers, and Domain Name.

Examples

The following command displays IP addresses using the various keywords:

```
controller# show ip
```

ID	IP Address	NetMask	Type
0	192.168.10.2	255.255.255.0	Static

IP Addresses(1 entry)

Interface Number	IP Address	NetMask	Gateway Address	Assign-
ment Type	Interface Mode			
1	172.26.0.53	255.255.240.0	172.26.0.1	DHCP

active

IP Addresses(1 entry)

```
controller# show ip default-gateway
192.168.10.1
controller# show ip dhcp-server
```

```
10.0.0.10
controller# show ip dns-server
DNS Server
```

```
10.0.0.10
      DNS Server Table(1 entry)
controller# show ip domainname
fortinet.com
```

show ipv6-neighbor

Displays the IPV6 neighbor table.

Syntax `show ipv6-neighbor`

Command Mode Global configuration

Default None

Usage Use this command to display the IPV6 neighbor table.

Examples MC3200(15)# `show ipv6-neighbor`

Related Commands [*ipv6-neighbor-discovery-optimization*](#) **on page 280**

show second_interface_status

Displays the FastEthernet interface 2 redundant mode status

Syntax

`show second_interface_status`

Command Mode

Privileged EXEC mode

Default

NA

Usage

Shows the status of the second FastEthernet interface, when configured in redundant mode, acting as a backup for the first interface on the controller.

Related Commands

- [interface FastEthernet](#) on page 264
- [type](#) on page 309
- [show interfaces FastEthernet controller](#) on page 297

static-route

Allows you to create and configure a Static Route.

Syntax

static-route <*name*>

name The name of the route to be modified or created.

Command Mode

Global configuration

Default

NA

Usage

This command is used to access static route properties and make changes by using the other commands documented in this chapter. All static route-based commands are performed while in static route configuration mode.

Examples

```
default(15)# configure terminal
default(15)(config)# static-route stat
default(15)(config-static-route)#
```

Related Commands

- [\(config-static-route\) interface on page 307](#)
- [\(config-static-route\) ip on page 308](#)

(config-static-route) interface

Specifies the Ethernet interface to be used by the route.

Syntax

interface fastEthernet <interface>

interface

Specify **primary** or **secondary** interface as desired.

Command Mode

Static Route configuration

Default

Primary

Usage

This command is used to specify the Ethernet interface used by the current Static Route. Users can select either the primary or secondary interface.

Examples

```
default(15)# configure terminal
default(15)(config)# static-route stat
default(15)(config-static-route)# interface fastEthernet secondary
default(15)(config-static-route)#
```

Related Commands

- [static-route](#) on page 306
- [\(config-static-route\) ip](#) on page 308

(config-static-route) ip

Specifies the IP address and subnet mask to be used by the route.

Syntax

ip address <ip> <subnet>

ip

The IP address in 255.255.255.255 notation.

subnet

The subnet mask in 255.255.255.255 notation.

Command Mode

Static Route configuration

Default

NA

Usage

This command is used to specify the IP address and subnet mask used for the current Static Route.

Examples

```
default(15)# configure terminal
default(15)(config)# static-route stat
default(15)(config-static-route)# ip address 192.168.14.0 255.255.255.0
default(15)(config-static-route)#
```

Related Commands

- [static-route](#) on page 306
- [\(config-static-route\) interface](#) on page 307

type

Configures the FastEthernet interface usage type.

Syntax

`type active`
`type redundant`

active	Sets the interface as a fully-functional FastEthernet interface. Can be used for interface 1 or 2.
redundant	Sets the interface as a backup to FastEthernet interface 1. Can only be used when the interface index is 2.

Command Mode

FastEthernet interface configuration mode

Default

NA

Usage

This command determines how the FastEthernet interface is used. The **type** options are **active** and **redundant**, and the usage is dependent on the port being configured. The default interface 1 must be configured as **active**, but interface 2 may be configured as **active** or **redundant**.



The first Ethernet interface will be treated as the default interface. The responsibility of the default interface is to pass wireless tunnel traffic between the APs and the controller. In addition to the general support of GRE and VLAN, the default interface will also be the designated management interface for the controller, providing support for Management access traffic via SSH and HTTPS.

If the second interface is configured as **redundant**, it will serve as a backup interface to the first interface in a spanning tree configuration. This means that it will be idle as long as the first interface is functional and will perform all functions of the first interface if the first interface fails. In this configuration, the first interface must be set with a static IP address.

If the second interface is configured as **active**, it can be configured as a separate interface that can support an additional configuration (for example to support GRE tunneling while the first interface is configured for VLANs).

It is implicit in the configuration of redundant mode that the second Ethernet interface should be connected to a switch port in which it can perform the same functions as the default

Ethernet interface. Such a configuration can be better thought of as a spanning tree network setup.



Note that APs cannot be configured to discover the controller via the IP address assigned to the second interface. The controller's bonding mode must be set to dual or none (based on the controller model) before configuring the second interface for redundant or active mode. Refer to the FortiWLC (SD) Configuration Guide for more details.

Examples

The following commands configure Ethernet port 2 as an **active** interface that can be used to support a VLAN or GRE (Generic Routing Encapsulation) tunneling. The **ip address** specifies the IP address of interface followed by the associated netmask. The **gw** command specifies the gateway configuration, and is a mandatory field.

```
default# configure terminal
default(config)# interface FastEthernet 2
default(config-if-FastEth)# ip address 172.26.16.200 255.0.0.0
default(config-if-FastEth)# gw 172.26.16.1
default(config-if-FastEth)# type active
default(config-if-FastEth)# end
```

The following commands configure Ethernet interface 2 as a backup to Ethernet interface 1, as specified by **redundant** for the **type** option.

```
default# configure terminal
default(config)# interface FastEthernet 2
default(config-if-FastEth)# type redundant
default(config-if-FastEth)# end
```

Related Commands

- [gw on page 261](#)
- [interface FastEthernet on page 264](#)
- [ip address on page 266](#)
- [show interfaces FastEthernet controller on page 297](#)
- [show second_interface_status on page 305](#)

virtual-interface-profile

Allows you to create and configure a Virtual Interface Profile.

Syntax

virtual-interface-profile <*profile*>

profile

The name of the profile to be modified or created.

Command Mode

Global configuration

Default

NA

Usage

This command is used to access virtual interface profile properties and make changes by using the other commands documented in this chapter. All virtual interface-based commands are performed while in virtual interface configuration mode.

Examples

```
default(15)# configure terminal
default(15)(config)# virtual-interface-profile vip
default(15)(config-virtual-interface-profile)#
```

Related Commands

- [\(config-vip\) disable on page 312](#)
- [\(config-vip\) enable on page 313](#)
- [\(config-vip\) gateway on page 314](#)
- [\(config-vip\) ip on page 315](#)
- [\(config-vip\) show on page 316](#)

(config-vip) disable

Disables the current Virtual Interface Profile.

Syntax

disable

Command Mode

Virtual Interface Profile configuration

Default

Disabled

Usage

This command is used to disable the active Virtual Interface Profile.

Examples

```
default(15)# configure terminal
default(15)(config)# virtual-interface-profile vip
default(15)(config-virtual-interface-profile)# disable
default(15)(config-virtual-interface-profile)#
```

Related Commands

- [virtual-interface-profile](#) on page 311
- [\(config-vip\) enable](#) on page 313
- [\(config-vip\) gateway](#) on page 314
- [\(config-vip\) ip](#) on page 315
- [\(config-vip\) show](#) on page 316

(config-vip) enable

Enables the current Virtual Interface Profile.

Syntax

enable

Command Mode

Virtual Interface Profile configuration

Default

Disabled

Usage

This command is used to enable the active Virtual Interface Profile.

Examples

```
default(15)# configure terminal
default(15)(config)# virtual-interface-profile vip
default(15)(config-virtual-interface-profile)# enable
default(15)(config-virtual-interface-profile)#
```

Related Commands

- [virtual-interface-profile](#) on page 311
- [\(config-vip\) disable](#) on page 312
- [\(config-vip\) gateway](#) on page 314
- [\(config-vip\) ip](#) on page 315
- [\(config-vip\) show](#) on page 316

(config-vip) gateway

Specifies the gateway address to be used for the current Virtual Interface Profile.

Syntax

gateway <ip>

ip

The IP address in 255.255.255.255 notation.

Command Mode

Virtual Interface Profile configuration

Default

NA

Usage

This command is used to set the gateway address for the active Virtual Interface Profile. This address must be entered in standard IP notation: 255.255.255.255.

Examples

```
default(15)# configure terminal
default(15)(config)# virtual-interface-profile vip
default(15)(config-virtual-interface-profile)# gateway 192.168.14.1
default(15)(config-virtual-interface-profile)#
```

Related Commands

- [virtual-interface-profile](#) on page 311
- [\(config-vip\) disable](#) on page 312
- [\(config-vip\) enable](#) on page 313
- [\(config-vip\) ip](#) on page 315
- [\(config-vip\) show](#) on page 316

(config-vip) ip

Specifies the subnet IP address and subnet mask to be used for the current Virtual Interface Profile.

Syntax

ip address <ip> <subnet>

<i>ip</i>	The IP address in 255.255.255.255 notation.
<i>subnet</i>	The subnet mask in 255.255.255.255 notation.

Command Mode

Virtual Interface Profile configuration

Default

NA

Usage

This command is used to set the subnet IP address and subnet mask for the active Virtual Interface Profile. This addresses must be entered in standard IP notation: 255.255.255.255.

Examples

```
default(15)# configure terminal
default(15)(config)# virtual-interface-profile vip
default(15)(config-virtual-interface-profile)# ip address 192.168.14.0
255.255.255.0
default(15)(config-virtual-interface-profile)#
```

Related Commands

- [virtual-interface-profile on page 311](#)
- [\(config-vip\) disable on page 312](#)
- [\(config-vip\) enable on page 313](#)
- [\(config-vip\) gateway on page 314](#)
- [\(config-vip\) show on page 316](#)

(config-vip) show

Allows you to display the current Virtual Interface Profile being modified.

Syntax

show context

Command Mode

Virtual Interface Profile configuration

Default

NA

Usage

This command is used to view the active Virtual Interface Profile.

Examples

```
default(15)# configure terminal
default(15)(config)# virtual-interface-profile vip
default(15)(config-virtual-interface-profile)# show context
Virtual Interface Profile Name: vip
default(15)(config-virtual-interface-profile)#
```

Related Commands

- [virtual-interface-profile](#) on page 311
- [\(config-vip\) disable](#) on page 312
- [\(config-vip\) enable](#) on page 313
- [\(config-vip\) gateway](#) on page 314
- [\(config-vip\) ip](#) on page 315

8 VLAN Commands

FortiWLC (SD) provides commands for configuring both virtual LAN (VLANs) and Generic Routing Encapsulation (GRE) tunnels to facilitate the separation of traffic using a logical rather than physical constraints. VLANs and GRE tunnels can coexist within any given network, logically segmenting traffic by organization or function. In this way, all systems used by a given organization can be interconnected, independent of physical location. This has the benefit of limiting the broadcast domain and increasing security. The commands to create and configure GRE tunnels and VLANs are:

- [*dhcp-server*](#) **on page 319**
- [*\(config-dhcp-server\) disable*](#) **on page 321**
- [*\(config-dhcp-server\) dns-server-primary*](#) **on page 322**
- [*\(config-dhcp-server\) dns-server-secondary*](#) **on page 323**
- [*\(config-dhcp-server\) domain-name*](#) **on page 325**
- [*\(config-dhcp-server\) enable*](#) **on page 326**
- [*\(config-dhcp-server\) ip-pool*](#) **on page 327**
- [*\(config-dhcp-server\) lease-time*](#) **on page 329**
- [*\(config-dhcp-server\) netbios-server-primary*](#) **on page 331**
- [*\(config-dhcp-server\) netbios-server-secondary*](#) **on page 333**
- [*\(config-dhcp-server\) option-43*](#) **on page 335**
- [*\(config-dhcp-server\) show*](#) **on page 337**
- [*\(config-dhcp-server\) vlan*](#) **on page 338**
- [*\(config-dhcp-server\) virtual-interface-profile*](#) **on page 340**
- [*gre*](#) **on page 342**
- [*interface FastEthernet controller*](#) **on page 344**
- [*ip remote-external-address*](#) **on page 346**
- [*ip tunnel-ip-address*](#) **on page 347**
- [*show dhcp-server*](#) **on page 348**
- [*show gre*](#) **on page 350**
- [*show dhcp-lease*](#) **on page 351**

- [show vlan](#) on page 352
- [test gre](#) on page 354
- [vlan](#) on page 355
- [wapi-server](#) on page 356

dhcp-server

Provides access to configuring the controller-based DHCP server.

Syntax

dhcp-server <name>

name The name for the DHCP server to be modified or created.

Command Mode

Global configuration

Default

NA

Usage

This command is used to access the controller-based DHCP server's configuration mode. All DHCP-based commands must be executed from within this mode.

Example

```
default(15)# configure terminal
default(15)(config)# dhcp-server dhcp1
default(15)(config-dhcp-server)#
```

Related Commands

- [show dhcp-server on page 348](#)
- [show dhcp-lease on page 351](#)
- [\(config-dhcp-server\) disable on page 321](#)
- [\(config-dhcp-server\) dns-server-primary on page 322](#)
- [\(config-dhcp-server\) dns-server-secondary on page 323](#)
- [\(config-dhcp-server\) domain-name on page 325](#)
- [\(config-dhcp-server\) enable on page 326](#)
- [\(config-dhcp-server\) ip-pool on page 327](#)
- [\(config-dhcp-server\) lease-time on page 329](#)
- [\(config-dhcp-server\) netbios-server-primary on page 331](#)
- [\(config-dhcp-server\) netbios-server-secondary on page 333](#)
- [\(config-dhcp-server\) option-43 on page 335](#)
- [\(config-dhcp-server\) show on page 337](#)

- [\(config-dhcp-server\) vlan](#) on **page 338**
- [\(config-dhcp-server\) virtual-interface-profile](#) on **page 340**

(config-dhcp-server) disable

Disables the current DHCP Server.

Syntax

disable

Command Mode

DHCP Server configuration

Default

Disabled

Usage

This command is used to disable the active DHCP Server.

Examples

```
default(15)# configure terminal
default(15)(config)# dhcp-server dhcp1
default(15)(config-dhcp-server)# disable
default(15)(config-dhcp-server)#
```

Related Commands

- [dhcp-server on page 319](#)
- [\(config-dhcp-server\) dns-server-primary on page 322](#)
- [\(config-dhcp-server\) dns-server-secondary on page 323](#)
- [\(config-dhcp-server\) domain-name on page 325](#)
- [\(config-dhcp-server\) enable on page 326](#)
- [\(config-dhcp-server\) ip-pool on page 327](#)
- [\(config-dhcp-server\) lease-time on page 329](#)
- [\(config-dhcp-server\) netbios-server-primary on page 331](#)
- [\(config-dhcp-server\) netbios-server-secondary on page 333](#)
- [\(config-dhcp-server\) option-43 on page 335](#)
- [\(config-dhcp-server\) show on page 337](#)
- [\(config-dhcp-server\) vlan on page 338](#)
- [\(config-dhcp-server\) virtual-interface-profile on page 340](#)

(config-dhcp-server) dns-server-primary

Configures the primary DNS server for the current DHCP Server.

Syntax

dns-server-primary <IP>

IP The IP of the desired DNS server.

Command Mode

DHCP Server configuration

Default

NA

Usage

This command is used to enter the IP address to be used by the DHCP Server for a primary DNS server.

Examples

```
default(15)# configure terminal
default(15)(config)# dhcp-server dhcp1
default(15)(config-dhcp-server)# dns-server-primary 192.168.14.14
default(15)(config-dhcp-server)#
```

Related Commands

- [dhcp-server on page 319](#)
- [\(config-dhcp-server\) disable on page 321](#)
- [\(config-dhcp-server\) dns-server-secondary on page 323](#)
- [\(config-dhcp-server\) domain-name on page 325](#)
- [\(config-dhcp-server\) enable on page 326](#)
- [\(config-dhcp-server\) ip-pool on page 327](#)
- [\(config-dhcp-server\) lease-time on page 329](#)
- [\(config-dhcp-server\) netbios-server-primary on page 331](#)
- [\(config-dhcp-server\) netbios-server-secondary on page 333](#)
- [\(config-dhcp-server\) option-43 on page 335](#)
- [\(config-dhcp-server\) show on page 337](#)
- [\(config-dhcp-server\) vlan on page 338](#)
- [\(config-dhcp-server\) virtual-interface-profile on page 340](#)

(config-dhcp-server) dns-server-secondary

Configures the secondary DNS server for the current DHCP Server.

Syntax

dns-server-secondary <IP>

IP

The IP of the desired DNS server.

Command Mode

DHCP Server configuration

Default

NA

Usage

This command is used to enter the IP address to be used by the DHCP Server for a secondary DNS server.

Examples

```
default(15)# configure terminal
default(15)(config)# dhcp-server dhcp1
default(15)(config-dhcp-server)# dns-server-secondary 192.168.17.17
default(15)(config-dhcp-server)#
```

Related Commands

- [dhcp-server on page 319](#)
- [\(config-dhcp-server\) disable on page 321](#)
- [\(config-dhcp-server\) dns-server-primary on page 322](#)
- [\(config-dhcp-server\) domain-name on page 325](#)
- [\(config-dhcp-server\) enable on page 326](#)
- [\(config-dhcp-server\) ip-pool on page 327](#)
- [\(config-dhcp-server\) lease-time on page 329](#)
- [\(config-dhcp-server\) netbios-server-primary on page 331](#)
- [\(config-dhcp-server\) netbios-server-secondary on page 333](#)
- [\(config-dhcp-server\) option-43 on page 335](#)
- [\(config-dhcp-server\) show on page 337](#)

- [\(config-dhcp-server\) vlan](#) **on page 338**
- [\(config-dhcp-server\) virtual-interface-profile](#) **on page 340**

(config-dhcp-server) domain-name

Configures the domain name used by the current DHCP Server.

Syntax

domain-name <name>

name The desired domain name.

Command Mode

DHCP Server configuration

Default

NA

Usage

This command is used to enter the domain name to be used by the DHCP Server.

Examples

```
default(15)# configure terminal
default(15)(config)# dhcp-server dhcp1
default(15)(config-dhcp-server)# domain-name sampledomain
default(15)(config-dhcp-server)#
```

Related Commands

- [dhcp-server on page 319](#)
- [\(config-dhcp-server\) disable on page 321](#)
- [\(config-dhcp-server\) dns-server-primary on page 322](#)
- [\(config-dhcp-server\) dns-server-secondary on page 323](#)
- [\(config-dhcp-server\) enable on page 326](#)
- [\(config-dhcp-server\) ip-pool on page 327](#)
- [\(config-dhcp-server\) lease-time on page 329](#)
- [\(config-dhcp-server\) netbios-server-primary on page 331](#)
- [\(config-dhcp-server\) netbios-server-secondary on page 333](#)
- [\(config-dhcp-server\) option-43 on page 335](#)
- [\(config-dhcp-server\) show on page 337](#)
- [\(config-dhcp-server\) vlan on page 338](#)
- [\(config-dhcp-server\) virtual-interface-profile on page 340](#)

(config-dhcp-server) enable

Enables the current DHCP Server.

Syntax

enable

Command Mode

DHCP Server configuration

Default

Disabled

Usage

This command is used to enable the active DHCP Server.

Examples

```
default(15)# configure terminal
default(15)(config)# dhcp-server dhcp1
default(15)(config-dhcp-server)# enable
default(15)(config-dhcp-server)#
```

Related Commands

- [dhcp-server on page 319](#)
- [\(config-dhcp-server\) disable on page 321](#)
- [\(config-dhcp-server\) dns-server-primary on page 322](#)
- [\(config-dhcp-server\) dns-server-secondary on page 323](#)
- [\(config-dhcp-server\) domain-name on page 325](#)
- [\(config-dhcp-server\) ip-pool on page 327](#)
- [\(config-dhcp-server\) lease-time on page 329](#)
- [\(config-dhcp-server\) netbios-server-primary on page 331](#)
- [\(config-dhcp-server\) netbios-server-secondary on page 333](#)
- [\(config-dhcp-server\) option-43 on page 335](#)
- [\(config-dhcp-server\) show on page 337](#)
- [\(config-dhcp-server\) vlan on page 338](#)
- [\(config-dhcp-server\) virtual-interface-profile on page 340](#)

(config-dhcp-server) ip-pool

Specifies the range of IPs that can be assigned by the DHCP server.

Syntax

ip-pool <start-ip> <end-ip>

start-ip The first IP that can be assigned.

end-ip The final IP that can be assigned.

Command Mode

DHCP Server configuration

Default

NA

Usage

This command is used to configure the range of IP addresses that are reserved for use by the current DHCP server. All IPs between the two entered as command line parameters will be available for use.

Examples

```
default(15)# configure terminal
default(15)(config)# dhcp-server dhcp1
default(15)(config-dhcp-server)# ip-pool 192.168.15.100 192.168.15.150
default(15)(config-dhcp-server)#
```

Related Commands

- [dhcp-server on page 319](#)
- [\(config-dhcp-server\) disable on page 321](#)
- [\(config-dhcp-server\) dns-server-primary on page 322](#)
- [\(config-dhcp-server\) dns-server-secondary on page 323](#)
- [\(config-dhcp-server\) domain-name on page 325](#)
- [\(config-dhcp-server\) enable on page 326](#)
- [\(config-dhcp-server\) lease-time on page 329](#)
- [\(config-dhcp-server\) netbios-server-primary on page 331](#)
- [\(config-dhcp-server\) netbios-server-secondary on page 333](#)
- [\(config-dhcp-server\) option-43 on page 335](#)

- *(config-dhcp-server) show on page 337*
- *(config-dhcp-server) vlan on page 338*
- *(config-dhcp-server) virtual-interface-profile on page 340*

(config-dhcp-server) lease-time

Specifies the duration of leases that are assigned by the DHCP server.

Syntax

lease-time <time>

time The duration of the lease (in seconds). Can range from 300-65535.

Command Mode

DHCP Server configuration

Default

NA

Usage

This command is used to configure the duration of the DHCP leases assigned by the current server. Lease times are entered in seconds and must be between 300 and 65535.

Examples

```
default(15)# configure terminal
default(15)(config)# dhcp-server dhcp1
default(15)(config-dhcp-server)# lease-time 3000
default(15)(config-dhcp-server)#
```

Related Commands

- [dhcp-server on page 319](#)
- [\(config-dhcp-server\) disable on page 321](#)
- [\(config-dhcp-server\) dns-server-primary on page 322](#)
- [\(config-dhcp-server\) dns-server-secondary on page 323](#)
- [\(config-dhcp-server\) domain-name on page 325](#)
- [\(config-dhcp-server\) enable on page 326](#)
- [\(config-dhcp-server\) ip-pool on page 327](#)
- [\(config-dhcp-server\) netbios-server-primary on page 331](#)
- [\(config-dhcp-server\) netbios-server-secondary on page 333](#)
- [\(config-dhcp-server\) option-43 on page 335](#)
- [\(config-dhcp-server\) show on page 337](#)
- [\(config-dhcp-server\) vlan on page 338](#)

- [\(config-dhcp-server\) virtual-interface-profile](#) **on page 340**

(config-dhcp-server) netbios-server-primary

Configures the primary netbios server for the current DHCP Server.

Syntax

`netbios-server-primary <IP>`

IP The IP of the desired netbios server.

Command Mode

DHCP Server configuration

Default

NA

Usage

This command is used to enter the IP address to be used by the DHCP Server for a primary netbios server.

Examples

```
default(15)# configure terminal
default(15)(config)# dhcp-server dhcp1
default(15)(config-dhcp-server)# netbios-server-primary 192.168.14.24
default(15)(config-dhcp-server)#
```

Related Commands

- [dhcp-server on page 319](#)
- [\(config-dhcp-server\) disable on page 321](#)
- [\(config-dhcp-server\) dns-server-primary on page 322](#)
- [\(config-dhcp-server\) dns-server-secondary on page 323](#)
- [\(config-dhcp-server\) domain-name on page 325](#)
- [\(config-dhcp-server\) enable on page 326](#)
- [\(config-dhcp-server\) ip-pool on page 327](#)
- [\(config-dhcp-server\) lease-time on page 329](#)
- [\(config-dhcp-server\) netbios-server-secondary on page 333](#)
- [\(config-dhcp-server\) option-43 on page 335](#)
- [\(config-dhcp-server\) show on page 337](#)

- [\(config-dhcp-server\) vlan](#) on **page 338**
- [\(config-dhcp-server\) virtual-interface-profile](#) on **page 340**

(config-dhcp-server) netbios-server-secondary

Configures the secondary netbios server for the current DHCP Server.

Syntax

netbios-server-secondary <IP>

IP

The IP of the desired netbios server.

Command Mode

DHCP Server configuration

Default

NA

Usage

This command is used to enter the IP address to be used by the DHCP Server for a secondary netbios server.

Examples

```
default(15)# configure terminal
default(15)(config)# dhcp-server dhcp1
default(15)(config-dhcp-server)# netbios-server-secondary 192.168.17.27
default(15)(config-dhcp-server)#
```

Related Commands

- [dhcp-server on page 319](#)
- [\(config-dhcp-server\) disable on page 321](#)
- [\(config-dhcp-server\) dns-server-primary on page 322](#)
- [\(config-dhcp-server\) dns-server-secondary on page 323](#)
- [\(config-dhcp-server\) domain-name on page 325](#)
- [\(config-dhcp-server\) enable on page 326](#)
- [\(config-dhcp-server\) ip-pool on page 327](#)
- [\(config-dhcp-server\) lease-time on page 329](#)
- [\(config-dhcp-server\) netbios-server-primary on page 331](#)
- [\(config-dhcp-server\) option-43 on page 335](#)
- [\(config-dhcp-server\) show on page 337](#)

- [\(config-dhcp-server\) vlan](#) on **page 338**
- [\(config-dhcp-server\) virtual-interface-profile](#) on **page 340**

(config-dhcp-server) option-43

Enables DHCP Option 43 configuration for the DHCP server.

Syntax

option-43 <hostname1>,<hostname2>

hostname1 The hostname or IP address of the controller that supports DHCP Option 43.

hostname2 Optionally, specify a second controller that supports DHCP Option 43.

Command Mode

DHCP Server configuration

Default

NA

Usage

This command is used to enable DHCP Option 43 support on the DHCP server. This function is used for vendor-specific AP operations; refer to AP documentation for details. Up to two controllers can be specified for Option 43 configuration.

Examples

```
default(15)# configure terminal
default(15)(config)# dhcp-server dhcp1
default(15)(config-dhcp-server)# option-43 172.15.182.36,176.27.3.45
default(15)(config-dhcp-server)#
```

Related Commands

- [dhcp-server on page 319](#)
- [\(config-dhcp-server\) disable on page 321](#)
- [\(config-dhcp-server\) dns-server-primary on page 322](#)
- [\(config-dhcp-server\) dns-server-secondary on page 323](#)
- [\(config-dhcp-server\) domain-name on page 325](#)
- [\(config-dhcp-server\) enable on page 326](#)
- [\(config-dhcp-server\) ip-pool on page 327](#)
- [\(config-dhcp-server\) lease-time on page 329](#)
- [\(config-dhcp-server\) netbios-server-primary on page 331](#)

- [\(config-dhcp-server\) netbios-server-secondary](#) on page 333
- [\(config-dhcp-server\) show](#) on page 337
- [\(config-dhcp-server\) vlan](#) on page 338
- [\(config-dhcp-server\) virtual-interface-profile](#) on page 340

(config-dhcp-server) show

Allows you to display the current DHCP server being modified.

Syntax

show context

Command Mode

DHCP Server configuration

Default

NA

Usage

This command is used to view the active DHCP Server.

Examples

```
default(15)# configure terminal
default(15)(config)# dhcp-server dhcp1
default(15)(config-dhcp-server)# show context
DHCP Server Pool Name: dhcp1
default(15)(config-dhcp-server)#
```

Related Commands

- [dhcp-server on page 319](#)
- [\(config-dhcp-server\) disable on page 321](#)
- [\(config-dhcp-server\) dns-server-primary on page 322](#)
- [\(config-dhcp-server\) dns-server-secondary on page 323](#)
- [\(config-dhcp-server\) domain-name on page 325](#)
- [\(config-dhcp-server\) enable on page 326](#)
- [\(config-dhcp-server\) ip-pool on page 327](#)
- [\(config-dhcp-server\) lease-time on page 329](#)
- [\(config-dhcp-server\) netbios-server-primary on page 331](#)
- [\(config-dhcp-server\) netbios-server-secondary on page 333](#)
- [\(config-dhcp-server\) option-43 on page 335](#)
- [\(config-dhcp-server\) vlan on page 338](#)
- [\(config-dhcp-server\) virtual-interface-profile on page 340](#)

(config-dhcp-server) vlan

Specifies the name of the VLAN assigned to the DHCP Server.

Syntax

vlan <name>

name The name of the VLAN.

Command Mode

DHCP Server configuration

Default

NA

Usage

This command is used to configure the name of the VLAN assigned to the DHCP server. Note that this option is only available when the controller is operating in L2 Routing mode.

Examples

```
default(15)# configure terminal
default(15)(config)# dhcp-server dhcp1
default(15)(config-dhcp-server)# vlan v1
default(15)(config-dhcp-server)#
```

Related Commands

- [dhcp-server on page 319](#)
- [\(config-dhcp-server\) disable on page 321](#)
- [\(config-dhcp-server\) dns-server-primary on page 322](#)
- [\(config-dhcp-server\) dns-server-secondary on page 323](#)
- [\(config-dhcp-server\) domain-name on page 325](#)
- [\(config-dhcp-server\) enable on page 326](#)
- [\(config-dhcp-server\) ip-pool on page 327](#)
- [\(config-dhcp-server\) lease-time on page 329](#)
- [\(config-dhcp-server\) netbios-server-primary on page 331](#)
- [\(config-dhcp-server\) netbios-server-secondary on page 333](#)
- [\(config-dhcp-server\) option-43 on page 335](#)
- [\(config-dhcp-server\) show on page 337](#)

- [\(config-dhcp-server\) virtual-interface-profile](#) **on page 340**

(config-dhcp-server) virtual-interface-profile

Specifies the name of the Virtual Interface Profile assigned to the DHCP Server.

Syntax

virtual-interface-profile <name>

name The name assigned to the Virtual Interface Profile.

Command Mode

DHCP Server configuration

Default

NA

Usage

This command is used to configure the name of the Virtual Interface Profile assigned to the DHCP server.

Examples

```
default(15)# configure terminal
default(15)(config)# dhcp-server dhcp1
default(15)(config-dhcp-server)# virtual-interface-profile vint1
default(15)(config-dhcp-server)#
```

Related Commands

- [dhcp-server on page 319](#)
- [\(config-dhcp-server\) disable on page 321](#)
- [\(config-dhcp-server\) dns-server-primary on page 322](#)
- [\(config-dhcp-server\) dns-server-secondary on page 323](#)
- [\(config-dhcp-server\) domain-name on page 325](#)
- [\(config-dhcp-server\) enable on page 326](#)
- [\(config-dhcp-server\) ip-pool on page 327](#)
- [\(config-dhcp-server\) lease-time on page 329](#)
- [\(config-dhcp-server\) netbios-server-primary on page 331](#)
- [\(config-dhcp-server\) netbios-server-secondary on page 333](#)
- [\(config-dhcp-server\) option-43 on page 335](#)

- [\(config-dhcp-server\) show](#) **on page 337**
- [\(config-dhcp-server\) vlan](#) **on page 338**

gre

Names the GRE tunnel profile and enters GRE configuration submenu.

Syntax

gre <name>

name Name of the GRE tunnel profile.

Command Mode

Global configuration

Default

NA

Usage

This command is used to specify the name of the GRE tunnel profile and enter the GRE configuration submenu, where details of the GRE tunnel are specified. The name of this profile is also used for the other part of the configuration, where it specifies the GRE profile in the ESSID profile.

The following points should be noted when configuring a GRE tunnel:

- The DHCP relay pass-through flag always should be off for a GRE tunnel. This ensures the DHCP relay is always on and hence the DHCP request packets are forwarded to the DHCP Server specified by DHCP Server IP Address.
- DHCP traffic associated with users connecting to a GRE tunnel are relayed to the configured DHCP Server located at the remote location through the associated GRE tunnel.
- Only IPv4 support is provided for GRE tunneling.

Examples

The following example shows how the command is used for configuring a GRE tunnel profile on the second FastEthernet interface, where the IP address of the tunnel's local endpoint is 13.13.13.13 and the remote endpoint is 172.27.0.206, and the DHCP server is at 10.0.0.12:

```
default(config)# gre guest
default(config-gre)# interface FastEthernet controller 2
default(config-gre)# ip tunnel-ip-address 13.13.13.13 255.255.0.0
default(config-gre)# ip remote-external-address 172.27.0.206
default(config-gre)# ip dhcp-override
default(config-gre)# ip dhcp-server 10.0.0.12
```

```
default(config-gre)# end
```

Related Commands

- [ssid](#) on page 547
- [interface FastEthernet](#) on page 264
- [ip dhcp-server](#) on page 272
- [ip remote-external-address](#) on page 346
- [show gre](#) on page 350
- [test gre](#) on page 354

interface FastEthernet controller

Selects the configured FastEthernet interface for use with the GRE tunnel.

Syntax

```
interface FastEthernet controller <number>
```

number The interface number of the controller to be configured, either 1 or 2.

Command Mode

GRE configuration submode

Default

NA

Usage

This command is used to specify the controller interface that is to be used by the GRE tunnel being configured. The interface that is selected (either the controller FastEthernet interface 1 or 2) must already be configured—either by the **setup** command or by the **interface FastEthernet** command. The interface must be in active mode and have an assigned IP address.

Examples

The following example shows how the command is used for configuring a GRE tunnel profile on the second FastEthernet interface, where the IP address of the tunnel's local endpoint is 13.13.13.13 and the remote endpoint is 172.27.0.206, and the DHCP server is at 10.0.0.12:

```
default(config)# gre guest
default(config-gre)# interface FastEthernet controller 2
default(config-gre)# ip tunnel-ip-address 13.13.13.13 255.255.0.0
default(config-gre)# ip remote-external-address 172.27.0.206
default(config-gre)# ip dhcp-override
default(config-gre)# ip dhcp-server 10.0.0.12
default(config-gre)# end
```

Related Commands

- [gre on page 342](#)
- [interface FastEthernet on page 264](#)
- [ip dhcp-server on page 272](#)
- [ip remote-external-address on page 346](#)

- *show gre on page 350*
- *test gre on page 354*

ip remote-external-address

Configures the IP address of the remote endpoint of a GRE tunnel.

Syntax

ip remote-external-address <address>

address IP address of the GRE tunnel remote endpoint.

Command Mode

GRE configuration submode

Default

Usage

This command is used to specify the address of the remote endpoint of the GRE tunnel that is being created. This IP address must be unique within the configuration to be successful.

Examples

The following example shows how the command is used for configuring a GRE tunnel profile on the second FastEthernet interface, where the IP address of the tunnel's local endpoint is 13.13.13.13 and the remote endpoint is 172.27.0.206, and the DHCP server is at 10.0.0.12:

```
default(config)# gre guest
default(config-gre)# interface FastEthernet controller 2
default(config-gre)# ip tunnel-ip-address 13.13.13.13 255.255.0.0
default(config-gre)# ip remote-external-address 172.27.0.206
default(config-gre)# ip dhcp-override
default(config-gre)# ip dhcp-server 10.0.0.12
default(config-gre)# end
```

Related Commands

- [gre on page 342](#)
- [interface FastEthernet on page 264](#)
- [ip dhcp-server on page 272](#)
- [ip tunnel-ip-address on page 347](#)
- [show gre on page 350](#)
- [test gre on page 354](#)

ip tunnel-ip-address

Configures the IP address of the GRE tunnel.

Syntax

```
ip tunnel-ip-address <address>
```

address IP address of the GRE tunnel.

Command Mode

GRE configuration submode

Default

Usage

This command is used to specify the address of the GRE tunnel that is being created. This IP address must be unique within the configuration to be successful.

Examples

The following example shows how the command is used for configuring a GRE tunnel profile on the second FastEthernet interface, where the IP address of the tunnel's local endpoint is 13.13.13.13 and the remote endpoint is 172.27.0.206, and the DHCP server is at 10.0.0.12:

```
default(config)# gre guest
default(config-gre)# interface FastEthernet controller 2
default(config-gre)# ip tunnel-ip-address 13.13.13.13 255.255.0.0
default(config-gre)# ip remote-external-address 172.27.0.206
default(config-gre)# ip dhcp-override
default(config-gre)# ip dhcp-server 10.0.0.12
default(config-gre)# end
```

Related Commands

- [gre on page 342](#)
- [interface FastEthernet on page 264](#)
- [ip dhcp-server on page 272](#)
- [ip remote-external-address on page 346](#)
- [show gre on page 350](#)
- [test gre on page 354](#)

show dhcp-server

Displays the current configuration of the controller-based DHCP server.

Syntax

```
show dhcp-server
show dhcp-server <VLAN>
```

VLAN	ID for a specific VLAN on which the DHCP server is enabled.
------	---

Command Mode

Global configuration

Default

NA

Usage

Entering this command displays the configured properties of the DHCP server:

- Enabled/Disabled
- Subnet
- IP range for clients
- Subnet mask
- Broadcast IP address
- Gateway IP address
- Maximum lease duration
- IP for the DNS (maximum of 2)
- IP for the Netbios server (maximum of 2)

Examples

```
default(15)# show dhcp-server
```

Tag	State	Lease time	DHCP IP	Subnet	DHCP Netmask	Gateway	IP
Pool	start	IP Pool end		Domain Name		DNS Server1	
102	enable	3600	192.168.102.0		255.255.255.0	192.168.102.1	
192.168.102.25		192.168.102.50				0.0.0.0	

Internal DHCP server configuration(1 entry)


```
default(15)# show dhcp-server 102
```

Internal DHCP server configuration

```
Tag (0 for default)      : 102
State                     : enable
Lease Time (in Seconds)  : 3600
IP Subnet                 : 192.168.102.0
Netmask                   : 255.255.255.0
Gateway                  : 192.168.102.1
IP Pool start             : 192.168.102.25
IP Pool end               : 192.168.102.50
Domain Name               :
DNS Server1               : 0.0.0.0
DNS Server2               : 0.0.0.0
Netbios Server1           : 0.0.0.0
Netbios Server2           : 0.0.0.0
```

Related Commands

- [dhcp-server](#) on page 319
- [show dhcp-lease](#) on page 351

show gre

Displays configured GRE tunnel information.

Syntax

`show gre <gre>`

gre Name of the GRE tunnel for which to show detailed information

Command Mode

Privileged EXEC

Default

NA

Usage

To see details about a GRE tunnel configuration, use the **show gre** command.

Examples

```
default# show gre
```

```
GRE NameRemote External AddressTunnel IP addressTunnel IP NetmaskLocal  
External
```

```
vlan1172.27.0.16212.12.12.12255.255.0.01
```

```
gre1172.27.0.20613.13.13.13255.255.0.02
```

```
GRE Configuration(2 entries)
```

Related Commands

- [gre on page 342](#)
- [interface FastEthernet on page 264](#)
- [ip dhcp-server on page 272](#)
- [ip remote-external-address on page 346](#)
- [ip tunnel-ip-address on page 347](#)
- [test gre on page 354](#)

show dhcp-lease

Displays the current DHCP lease information for the controller-based DHCP server.

Syntax

show dhcp-lease <option> <VLAN>

option	The desired parameter to be displayed. Can show statistics (using the <i>stats</i> parameter) or VLAN information (using the <i>vlan</i> option).
VLAN	ID for the VLAN on which the DHCP server is active. Only used when <i>vlan</i> is specified for the <i>option</i> field.

Command Mode

Privileged EXEC

Default

NA

Usage

Entering this command displays a list of all DHCP clients and the IP addresses assigned to them as well as the duration for each assignment.

Examples

default(15)# **show dhcp-lease vlan 102**

Related Commands

- [dhcp-server on page 319](#)
- [show dhcp-server on page 348](#)

show vlan

Displays configured VLAN information.

Syntax

```
show vlan
show vlan <vlan>
show vlan ess-profile
```

vlan Name of the VLAN for which to show detailed information

Command Mode

Privileged EXEC

Default

All configured VLANs are displayed.

Usage

To see more details about a specific VLAN, specify the VLAN name when using the **show vlan** command. To view which VLANs are mapped to which ESS profiles, use the **show vlan ess-profile** command. This function is used when Multicast is enabled.

Examples

The following commands displays all configured VLANs:

```
controller# show vlan
VLAN Configuration  VLAN Name Tag  IP Address      NetMask      Default
Gateway

my_vlan              3   0.0.0.0        0.0.0.0        0.0.0.0
guests               1   0.0.0.0        0.0.0.0        0.0.0.0
```

The following command shows detailed configuration information for the guests VLAN.

```
controller# show vlan guests
VLAN Configuration

VLAN Name           : guests
Tag                  : 1
IP Address           : 0.0.0.0
```

```
Netmask : 0.0.0.0
IP Address of the Default Gateway : 0.0.0.0
Override Default DHCP Server Flag : off
DHCP Server IP Address : 0.0.0.0
DHCP Relay Pass-Through : on
controller#
```

The following command shows the Multicast capabilities for each VLAN and ESS in use.

```
controller# show vlan ess-profile
```

VLAN Name	VLAN Tag	ESS Profile	Multicast	IPv6	AirFortress	Apple-Talk
-----	0	corp-mixed-peap	off	off	off	off
-----	0	corp-mixed-psk	off	off	off	off
-----	0	corp-wpa2peap	off	off	off	off
-----	0	corp-wpa2psk	on	off	off	off
-----	0	corp-wpapeap	off	off	off	off
-----	0	corp-wpapsk	off	off	off	off
-----	0	ph	off	on	off	off
Qa-Vlan-US	30	phone	on	off	off	off
captive-portal-g	9	guest	off	off	off	off

VLAN Ess Bonding(9)

Related Commands

vlan on page 355

test gre

Tests the GRE tunnel.

Syntax

```
test gre <gre_name>  
test gre <gre_name> <ip_address>
```

gre_name	GRE Profile name
ip_address	The IP address of the machine that is connected behind the tunnel (optional).

Command Mode

Privileged EXEC

Default

NA

Usage

To check the status of the a GRE tunnel, use the **test gre** command. The command will ping the IP address of the remote endpoint

Examples

To check the status of the GRE tunnel, use the example command:

```
default# test gre guest 13.13.13.13
```

Related Commands

- [gre on page 342](#)
- [interface FastEthernet on page 264](#)
- [ip dhcp-server on page 272](#)
- [ip remote-external-address on page 346](#)
- [ip tunnel-ip-address on page 347](#)
- [show gre on page 350](#)

vlan

Creates a VLAN and enters VLAN configuration mode.

Syntax

```
vlan <name>  
vlan <name> <tag id>
```

<i>name</i>	String of up to 16 alphanumeric characters long. Do not use spaces.
<i>tag id</i>	Tag number of the VLAN. Must be a value from 1 through 4,094.

Command Mode

Global configuration

Default

NA

Usage

You can create up to 512 VLANs for FortiWLC (SD).

Examples

The following commands assign the name *engineering* to a VLAN with a tag number of 42 and then shows help for the vlan configuration submode:

```
controller# vlan engineering tag 42  
controller(config-vlan)# ?  
default          Set various parameters to the default value.  
do               Executes an IOSCLI command.  
end              Save changes, and return to privileged EXEC mode.  
exit             Save changes, and return to global configuration  
mode.  
ip               Configure IP address, gateway, and DHCP server.  
no               Disabling various parameters.  
show            Displays various parameters.
```

Related Commands

[show vlan on page 352](#)

wapi-server

Configures the IP address used for the WLAN Authentication and Privacy Infrastructure.

Syntax

wapi-server <ip-address>

ip-address The IP Address for the WAPI server.

Command Mode

Global configuration

Default

NA

Usage

The WLAN Authentication and Privacy Infrastructure (WAPI) is a national standard for Wireless LANs in certain countries. For WAPI configurations, the controller must have the IP for the central Authentication Service Unit (ASU), which will verify that the wireless communication is permitted.

Examples

```
default(15)# configure terminal
default(15)(config)# wapi-server 192.168.14.14
default(15)(config-wapi-server)# end
```

Related Commands

9 Security Commands

Use these commands to configure and maintain WLAN security profiles:

- [*8021x-network-initiation*](#) **on page 361**
- [*access-list deny*](#) **on page 363**
- [*access-list deny import*](#) **on page 365**
- [*access-list permit*](#) **on page 367**
- [*access-list permit import*](#) **on page 369**
- [*administrator guest*](#) **on page 372**
- [*allowed-l2-modes*](#) **on page 373**
- [*app-visibility-policy*](#) **on page 375**
- [*app-visibility-custom-application*](#) **on page 377**
- [*sh service-summary Application-Visibility*](#) **on page 378**
- [*authentication-mode*](#) **on page 380**
- [*authentication-mode global*](#) **on page 382**
- [*authentication-type*](#) **on page 384**
- [*captive-portal*](#) **on page 388**
- [*captive-portal-auth-method*](#) **on page 390**
- [*cef*](#) **on page 392**
- [*certmgmt delete-ca*](#) **on page 395**
- [*certmgmt delete-csr*](#) **on page 397**
- [*certmgmt delete-server*](#) **on page 398**
- [*certmgmt export-ca*](#) **on page 400**
- [*certmgmt export-csr*](#) **on page 402**
- [*certmgmt export-server*](#) **on page 404**
- [*certmgmt list-ca*](#) **on page 406**
- [*certmgmt list-csr*](#) **on page 408**
- [*certmgmt list-server*](#) **on page 409**

- [change_mac_state](#) on page 416
- [change_mac_state](#) on page 416
- [change_mac_state](#) on page 416
- [change_mac_state](#) on page 416
- [description](#) on page 419
- [encryption-modes ccmp](#) on page 420
- [encryption-modes ccmp-tkip](#) on page 421
- [encryption-modes tkip](#) on page 422
- [encryption-modes wep128](#) on page 423
- [encryption-modes wep64](#) on page 424
- [firewall-capability](#) on page 425
- [firewall-filter-id](#) on page 426
- [firewall-filter-id-flow](#) on page 427
- [group-rekey interval](#) on page 428
- [import](#) on page 429
- [ip-address](#) on page 430
- [key](#) on page 431
- [key-rotation](#) on page 432
- [local-admin](#) on page 433
- [mac-delimiter](#) on page 435
- [macfiltering](#) on page 436
- [password](#) on page 437
- [password-type](#) on page 439
- [PMK-caching](#) on page 440
- [pmk caching](#) on page 441
- [port](#) on page 442
- [primary-tacacs-ip](#) on page 443
- [primary-tacacs-port](#) on page 445
- [primary-tacacs-secret](#) on page 447
- [privilege-level](#) on page 449
- [psk key](#) on page 452
- [radius-profile](#) on page 454
- [radius-server primary](#) on page 456
- [radius-server secondary](#) on page 457

- [reauth](#) on page 458
- [rekey period](#) on page 459
- [secondary-tacacs-ip](#) on page 460
- [secondary-tacacs-port](#) on page 462
- [secondary-tacacs-secret](#) on page 464
- [security-logging](#) on page 466
- [security-profile](#) on page 467
- [shared-authentication](#) on page 470
- [show aaa statistics](#) on page 472
- [show access-list deny](#) on page 473
- [show access-list permit](#) on page 474
- [show access-list state](#) on page 468
- [show air-shield](#) on page 475
- [show arp](#) on page 476
- [show authentication-mode](#) on page 478
- [show cef](#) on page 479
- [show local-admins](#) on page 480
- [show radius-profile](#) on page 482
- [show security-profile](#) on page 484
- [show ssl-server](#) on page 487
- [show web](#) on page 488
- [ssl-server associate](#) on page 492
- [ssl-server captive-portal](#) on page 493
- [ssl-server captive-portal-external_URL](#) on page 495
- [ssl-server port](#) on page 497
- [ssl-server radius-profile](#) on page 498
- [static-wep key](#) on page 501
- [static-wep key-index](#) on page 503
- [tunnel-termination](#) on page 504
- [vpn client](#) on page 505
- [\(config-vpn-client\) vpn-client-state](#) on page 506
- [\(config-vpn-client\) vpn-server-ip](#) on page 507
- [\(config-vpn-client\) vpn-server-port](#) on page 508
- [vpn server](#) on page 509

- [\(config-vpn\) encryption](#) on page 510
- [\(config-vpn\) ip-pool](#) on page 511
- [\(config-vpn\) port](#) on page 512
- [\(config-vpn\) subnet-mask](#) on page 513
- [\(config-vpn\) vpn-server-ip](#) on page 514
- [\(config-vpn\) vpn-server-state](#) on page 515
- [web custom](#) on page 516
- [web login-page](#) on page 518

8021x-network-initiation

Configures whether 802.1X authentication is initiated by the controller.

Syntax

```
8021x-network-initiation  
no 8021x-network-initiation
```

Command Mode

Security profile configuration

Default

802.1X network initiation is enabled.

Usage

802.1X network initiation allows the controller to initiate 802.1X authentication sessions. If 802.1X network initiation is disabled, the controller cannot initiate any aspect of 802.1X network authentication.

When 802.1X initialization is enabled, the authenticator proactively sends an EAP-REQUEST packet to the client. When disabled, the client sends an EAP-START packet to the authenticator (the controller).

Examples

The following command disables 802.1X network authentication:

```
controller(config-security)# no 8021x-network-initiation  
controller(config-security)#
```

Related Commands

- [allowed-l2-modes](#) on page 373
- [radius-profile](#) on page 454
- [radius-server primary](#) on page 456
- [radius-server secondary](#) on page 457

802.1x-termination

802.1x-Termination is provided by IOSCLI and Controller GUI, to perform configuration on per-security profile basis.

Syntax

```
802.1x-termination
PEAP TTLS
802.1x-termination PEAP
```

Command Mode

Security profile configuration

Default

Termination is off

Usage

802.1x termination allows the controller to terminate the PEAP/TTLS outer session on the controller. The inner MSCHAPv2 802.1x is handled by the backend radius server. This is useful when the radius server does not support PEAP or TTLS.

Examples

The following command disables the 802.1x termination:

```
controller(config-security)# no 802.1x-termination (peap/ttls)
controller(config-security)#
```



The following L2 Modes are supported only for the PEAP or TTLS authentication protocol:

- 802.1x
 - WPA
 - WPA2
 - Mixed
-

access-list deny

Adds the MAC address of a station to the deny list, which denies stations access to the network. Users may also add a brief description for the specified MAC.

Syntax

```
access-list deny <MAC-address>  
(config-acl-deny)# descr <description up to 40 characters>  
(config-acl-deny)# exit  
no access-list deny <MAC-address>  
no access-list deny all
```

MAC-address	MAC address of the station to be denied network access. Must be in hexadecimal format (nn:nn:nn:nn:nn:nn). A maximum of 1000 addresses are allowed.
all	When the all parameter is specified, all MAC addresses specified in the deny list are removed.

Command Mode

Global configuration

Default

NA

Usage

MAC address access list filtering controls access to the WLAN by permitting or denying access based on specific MAC addresses contained in an access or deny list. A deny list contains a list of client MAC addresses that are denied access to the WLAN.

A Deny ACL, which takes precedence over access that may be allowed through the RADIUS Server, can be used to immediately deny access to a station. It allows administrators to “black list” certain clients if they are misbehaving (for example, if they have a virus or are attacking other devices).

Before creating a permit or deny list, you must enable ACL using the **mac-filter-state** command before MAC addresses are permitted or denied. Only one list can be enabled at any given time; a permit and deny list cannot be enabled at the same time.

Use the **no** form to delete one entry or all entries in the list that denies stations access to the network.

Examples

The following command adds the MAC address `aa:11:aa:22:aa:33` to the deny list. It then adds DenyStation as the description for the MAC and displays the changes.

```
MC3200-5072(15)# configure terminal
MC3200-5072(15)(config)# access-list deny aa:11:aa:22:aa:33
MC3200-5072(15)(config-acl-deny)# descr DenyStation
MC3200-5072(15)(config-acl-deny)# end
MC3200-5072(15)# sh access-list deny
```

MAC Address	Description
aa:11:aa:22:aa:33	DenyStation

ACL Deny Access Configuration(1 entry)

```
MC3200-5072(15)#
```

Related Commands

- [access-list permit on page 367](#)
- [show access-list deny on page 473](#)

access-list deny import

Imports a text file of MAC addresses to be added to the deny list.

Syntax

access-list deny import <filename>

filename Name of the file that contains the MAC addresses to add to the deny list. The filename must follow UNIX file naming conventions.

Command Mode

Global configuration

Default

None

Usage

If you have a list of MAC addresses to add to the deny list, you can create a text file listing all the MAC addresses, and import the text file. Importing a file listing MAC addresses is an alternative to using the **access-list deny** command for each MAC address.

When creating the text file to be imported, only include one MAC address, in hexadecimal format (xx:xx:xx:xx:xx:xx), per line. For example, the contents of a text file to be imported might look like the following:

```
00:04:23:87:89:71
00:06:25:a7:e9:11
00:07:e9:15:69:40
00:0c:30:be:f8:19
00:0c:e6:09:46:64
00:0c:e6:12:07:41
00:0c:e6:bd:01:05
```

After creating a text file, you must transfer the file to the controller filesystem. From the CLI, use the **copy** command to transfer the file to the controller. Use the **dir** command to verify that the file is in the controller /images directory.

Examples

The following command imports a text file named *acl* and adds the MAC addresses in the file to the deny list:

```
controller(config)# access-list deny import acl
```

```
00:04:23:87:89:71
00:06:25:a7:e9:11
00:07:e9:15:69:40
00:0c:30:be:f8:19
00:0c:e6:09:46:64
00:0c:e6:12:07:41
00:0c:e6:bd:01:05
```

```
Successfully Added : 7
Duplicate Entries  : 0
Invalid Format      : 0
Entries Processed  : 7
controller(config)#
```

Related Commands

- [*copy on page 73*](#)
- [*dir on page 79*](#)
- [*show access-list deny on page 473*](#)
- [*show access-list state on page 468*](#)

access-list permit

Adds the MAC address of a station to the permit list, which permits stations access to the network. Users can also specify a brief description for the MAC.

Syntax

```
access-list permit <MAC-address>  
(config-acl-permit)# descr <description up to 40 characters>  
(config-acl-permit)# exit  
no access-list permit <MAC-address>  
no access-list permit all
```

MAC-address	MAC address of the station to be permitted network access. Must be in hexadecimal format (<i>nn:nn:nn:nn:nn:nn</i>). A maximum of 1000 addresses are allowed.
all	When the all parameter is specified, all MAC addresses specified in the permit list are removed.

Command Mode

Global configuration

Default

None

Usage

MAC filtering controls access to the WLAN by permitting or denying access based on specific MAC addresses. A permit list contains a list of MAC addresses that are permitted access to the WLAN. A deny list contains a list of MAC addresses that are denied access to the WLAN.

Before creating a permit or deny list, you must enable ACL by using the **mac-filter-state** command before MAC addresses are permitted or denied. Only one list can be enabled at any given time; a permit and deny list cannot be enabled at the same time. You can create permit and deny lists and disable them, making MAC filtering inactive.

Use the **no** form to delete one entry or all entries in the list that permits stations access to the network.

Examples

The following command adds the MAC address 11:11:11:11:22:22:33 to the permit list. It then enters "MyClient" for the description of that MAC and displays the new information.

```
MC3200-5072(15)# configure terminal
```

```
MC3200-5072(15)(config)# access-list permit 11:11:11:22:22:33
MC3200-5072(15)(config-acl-permit)# descr ?
<Descr> (10) Enter the Description to add.
```

```
MC3200-5072(15)(config-acl-permit)# descr MyClient
MC3200-5072(15)(config-acl-permit)# end
MC3200-5072(15)# sh access-list permit
```

```
MAC Address      Description
11:11:11:22:22:33  MyClient
ACL Allow Access Configuration(1 entry)
```

```
MC3200-5072(15)#
```

Related Commands

- [access-list permit import on page 369](#)
- [show access-list state on page 468](#)
- [show access-list permit on page 474](#)

access-list permit import

Imports a text file of MAC addresses to be added to the permit list.

Syntax

access-list permit import <filename>

filename

Name of the file that contains the MAC addresses to add to the permit list. The filename must follow UNIX file naming conventions.

Command Mode

Global configuration

Default

None

Usage

If you have a list of MAC addresses to add to the permit list, you can create a text file listing all the MAC addresses, and import the text file. Importing a file listing MAC addresses is an alternative to using the **access-list permit** command for each MAC address.

When creating the text file to be imported, only include one MAC address, in hexadecimal format (xx:xx:xx:xx:xx:xx), per line. For example, the contents of a text file to be imported might look like the following:

```
00:04:23:87:89:71
00:06:25:a7:e9:11
00:07:e9:15:69:40
00:0c:30:be:f8:19
00:0c:e6:09:46:64
00:0c:e6:12:07:41
00:0c:e6:bd:01:05
```

After creating a text file, you must transfer the file to the controller /images directory. From the CLI, use the **copy** command to transfer the file to the controller. Use the **dir** command to verify that the file is in the controller filesystem.

Examples

The following command imports a text file named *permit_acl* and adds the MAC addresses in the file to the permit list:

```
controller(config)# access-list permit import permit_acl
```

```
00:30:ab:1f:d4:b6
00:40:96:52:27:52
00:04:75:bb:94:48
00:0c:e6:bd:04:05
00:40:05:c5:ca:02
00:04:23:4b:68:6c
00:05:3c:08:c5:9e
```

```
Successfully Added : 7
Duplicate Entries  : 0
Invalid Format      : 0
Entries Processed  : 7
controller(config)#
```

Related Commands

- [copy](#) on page 73
- [dir](#) on page 79
- [show access-list permit](#) on page 474

mac-filter-state

Use this command to select one of the following the ACL environment.

Syntax

mac-filter-state <acl-environment-state>

- deny Deny List Enabled
- disabled ACL Disabled
- permit Permit List Enabled

administrator guest

Enables and disables the guest user account.

Syntax

```
administrator guest enable  
administrator guest disable
```

Command Mode

Global configuration

Default

Disabled in 4.0

Usage

The guest user account has been disabled by default in this 4.0 release. It can be enabled or disabled by using these CLI commands.

Examples

```
namecntrl# configure terminal  
namecntrl(config)# administrator guest enable  
namecntrl(config)# administrator guest disable  
namecntrl(config)#
```

Related Commands

- [captive-portal](#) on page 388
- [password](#) on page 437
- [password-type](#) on page 439

allowed-l2-modes

Defines the Layer 2 authentication mode that is permitted.

Syntax

```
allowed-l2-modes 802.1x
allowed-l2-modes clear
allowed-l2-modes mixed
allowed-l2-modes mixed_psk
allowed-l2-modes wep
allowed-l2-modes wpa
allowed-l2-modes wpa-psk
allowed-l2-modes wpa2
allowed-l2-modes wpa2-psk}
```

802.1x	Permits the IEEE 802.1X authentication mode.
clear	Does not specify an authentication mode.
mixed	Supports both WPA and WPA2 modes.
mixed-psk	Supports both WPA-PSK and WPA2-PSK modes.
wep	Permits the static WEP authentication mode.
wpa2	Permits the Wi-Fi Protected Access 2 (WPA2) security mode.
wpa2-psk	Permits the WPA2 Pre-Shared Key (PSK) key establishment method.
wpa	Permits the Wi-Fi Protected Access (WPA) security mode.
wpa-psk	Permits the WPA Pre-Shared Key (PSK) key establishment method.

Command Mode

Security Profile configuration

Default

The default permitted Layer 2 mode is **clear**, in which no authentication is enforced.

Usage

This command determines the Layer 2 authentication mode that is assigned to a security profile. Use this command to add 802.1X, WEP, WPA2, WPA2-PSK, WPA, or WPA-PSK authentication modes.



Only one Layer 2 method can be defined in each security profile.

WPA2-PSK or WPA-PSK can be used as an alternate key establishment method if WPA or WPA2 cannot be implemented using the 802.1X RADIUS server configuration. The WPA[2]-PSK implementation is a weaker form of security, and as such, is more suited to very small-scale sites.

Examples

The following command adds WPA2 as a permitted Layer 2 security mode:

```
controller(config-security)# allowed-l2-modes wpa2
controller(config-security)#
```

Related Commands

- [encryption-modes tkip](#) on page 422
- [encryption-modes wep128](#) on page 423
- [encryption-modes wep64](#) on page 424
- [radius-profile](#) on page 454

app-visibility-policy

Use this command as a start to creating an application visibility policy. Once you create a policy using this command, you can configure DPI control rules.

Syntax

`app-visibility-policy <policy-name>`

Options

Option	Description
advanced-detection	Enable/Disable Protocol/SubProtocol Detection.
apids	Configure APs. Adding access points: apids "<ap-id>: A" Adding access points groups: apids "<ap-group-name>: L"
appids	Configure Application IDs. Adding application: appids <application-ID>:<type>
description	Configure Policy Description.
essids	Configure ESSIDs. Adding ESS profiles: essids <essid-name>
owner	Owner of the profile. The owner is either controller or NMS. If the policy is created in the controller the owner is listed as controller
policy-order	Configure Application Policy Order. Policies are executed in the order they are displayed.
state	Enable/Disable for this Custom Application entry.
version	Version of the profile

Example

```
controller(15)# show application-visibility policy
```

Name	Enable	Applications	EssIds	AP Groups or APs
11	enable	2:A,3:B		apps1a
3:A				
123	enable	*		apps1a
143:A				
1232454	enable	2:A,3:B,4:B,5:B,6:A,7:A,8:A,9:A	apps1a	145:A
ALL	enable	*	apps1a	145:A

```

a          enable          *          appsla
123:L,143:A,145:A
rrer          enable          *          appsla1          1234:L
Application Visibility Policy(6)
controller(15)#

```

Legend

Legend	Description
A	When used for an application, it means to allow, detect, and monitor the application traffic.
B	Used to detect and block the application traffic
A	When used as an AP-ID, refers to adding an individual AP.
L	Used to add an ap-group to a policy.

app-visibility-custom-application

Use this command to create a policy for custom application. Custom applications are user-defined applications that are not part of the system defined applications. You can add a maximum of 32 applications in the controller and a maximum of 32 applications on Network Manager

Syntax

```
(config)# app-visibility-custom-application <policy-name>
(config-app-visibility-custom-application)# description <descriptive
text>
(config-app-visibility-custom-application)# url <app URL to block or mon-
itor>
```

Example

```
(config)# app-visibility-custom-application CustomApp-BBC
(config-app-visibility-custom-application)# description "To Monitor BBC
traffic"
(config-app-visibility-custom-application)# url www.bbc.com
(config-app-visibility-custom-application)# exit
# sh application-visibility custom-application
```

Name	Description	ID
CustomApp-BBC	To Monitor BBC traffic	10001

sh service-summary Application-Visibility

Example Use this command to monitor all your policies.

sh service-summary Application-Visibility

Feature	Type	Name	Value	ValueStr
Application-Visibility	Application	myspace	100	{"util":3006.76,"tx":6943001576,"rx":257651566}
Application-Visibility	Application	amazon_cloud	0	{"util":474.84,"tx":1093389603,"rx":43774451}
Application-Visibility	Application	facebook	0	{"util":184.00,"tx":421673492,"rx":18973696}
Application-Visibility	Application	twitter	0	{"util":164.58,"tx":358628579,"rx":35513363}
... <snipped> ...				
Application-Visibility	Station	08:11:96:7d:cf:80	0	{"util":286.78,"tx":657504303,"rx":29271859}
Application-Visibility	Station	24:77:03:80:a4:40	0	{"util":281.94,"tx":646183947,"rx":29009375}
Application-Visibility	Station	24:77:03:80:5f:54	0	{"util":280.23,"tx":645624714,"rx":25475052}
Application-Visibility	Station	24:77:03:85:b4:50	0	{"util":279.89,"tx":641592459,"rx":28689908}
Application-Visibility	EssId	stability	100	{"util":4055.84,"tx":9313033268,"rx":399999526}
Application-Visibility	AP	AP-109	100	{"util":4055.84,"tx":9313033268,"rx":399999526}

Service Data Summary(20 entries)

Use this command for a quick summary of top 10 applications

mc1500(15)# sh application-visibility application-summary

APPID	Name	Station	Counts	AP	ESS	Tx
Bytes	Rx Bytes	TxRx Bytes		Counts	Counts	
5	myspace	12	1	1	7274981850	
269918317	7544900167					
24	amazon_cloud	13		1	1	
1149026229	45994062	1195020291				

2	facebook	13	1	1	443832821
19962877	463795698				
8	twitter	13	1	1	375850987
37259491	413110478				
0	unknown	20	1	1	233565871
13899667	247465538				
70	amazon_shop	13	1	1	170637983
25318821	195956804				
41	linkedin	12	1	1	115430025
6896689	122326714				
32	youtube	13	1	1	3022484
304784	3327268				

Application Visibility Statistics Summary(8)

Use this command to view traffic trend

mc1500(15)# sh service-summary-trend Application-Visibility

Feature Value	ValueStr	Type	Name	StartTime	EndTime
Application-Visibility	Application	myspace		01/17/2009 01:00:00	01/17/2009 02:00:00
02:00:00	370191907	{ "util":254501.59,"tx":3561906268,"rx":140012805}			
Application-Visibility	Application	amazon_cloud		01/17/2009 01:00:00	01/17/2009 02:00:00
02:00:00	523131985	{ "util":35964.57,"tx":502700232,"rx":20431753}			
Application-Visibility	Application	twitter		01/17/2009 01:00:00	01/17/2009 02:00:00
02:00:00	221967525	{ "util":15259.95,"tx":202733592,"rx":19233933}			
Application-Visibility	Application	facebook		01/17/2009 01:00:00	01/17/2009 02:00:00
02:00:00	220636588	{ "util":15168.45,"tx":210304218,"rx":10332370}			
Application-Visibility	Application	unknown		01/17/2009 01:00:00	01/17/2009 02:00:00
02:00:00	113502079	{ "util":7803.10,"tx":106412520,"rx":7089559}			
Application-Visibility	Application	amazon_shop		01/17/2009 01:00:00	01/17/2009 02:00:00
02:00:00	106703142	{ "util":7335.69,"tx":93322094,"rx":13381048}			
Application-Visibility	Application	linkedin		01/17/2009 01:00:00	01/17/2009 02:00:00
02:00:00	58696435	{ "util":4035.30,"tx":55165018,"rx":3531417}			
... .. <snipped>					
Application-Visibility	Application	linkedin		01/17/2009 03:00:00	01/17/2009 04:00:00
04:00:00	121917540	{ "util":3824.43,"tx":114827231,"rx":7090309}			
Application-Visibility	Application	youtube		01/17/2009 03:00:00	01/17/2009 04:00:00
04:00:00	3187860	{ "util":100.00,"tx":2879796,"rx":308064}			

Service Data Summary Trend(24 entries)

authentication-mode

Command Mode with authentication commands to configure users.

Syntax

```
authentication-mode authentication-type local
authentication-mode authentication-type radius
authentication-mode primary-radius <profile_name>
authentication-mode secondary-radius <profile_name>
authentication-mode no-primary-radius
authentication-mode no-secondary-radius}
```

local	The local controller performs the user authentication. If authentication type is local for Captive Portal Authentication, only local guest users will be valid. Session-timeout and Activity time out controller values are used. Local is the default, and if that fails, Radius authentication is checked.
radius	A Radius server performs the user authentication. For Captive Portal Authentication, only Radius server users will be valid. Session-timeout and Activity time out Radius servervalues are used. Also if the Session timeout value is not configured in the Radius server, then the controller session timeout value will be used. If Radius fails, local authentication is not checked.
primary-radius	Specifies the name of the primary Radius server profile.
secondary-radius	Specifies the name of the secondary Radius server profile
profile_name	The profile name of the primary or secondary Radius server.
no-primary-radius	Disables the primary Radius server from performing authentication.
no-secondary-radius	Disables the secondary Radius server from performing authentication.

Default

none

Usage

Use this command to determine where authentication for Web users occurs. Authentication can be performed by the controller locally (using the local argument) or by a primary and secondary RADIUS server (using the radius argument) or by both (local and radius).

If the radius option is used, the name of the primary and optionally, the secondary, RADIUS server (specified in the profile_name argument) is used. The profile name for these servers must already have been created with the radius-profile command. If the radius option is specified, a user name and password with the controller's IP address must be created on the external RADIUS server for each userid to be authenticated.

Use no-primary-radius or no-secondary-radius arguments to disable the RADIUS server authentication configuration.

Examples

The following commands enable the local controller to perform user authentication:

```
default(config)# authentication-mode local
```

The following commands enable the primary Radius server configured in the Primary profile name to perform user authentication:

```
default(config)# authentication-mode radius
default(config)# authentication-mode radius-profile
default(config)# authentication-mode primary-radius Primary
```

The following commands disables the primary RADIUS server from performing user authentication and returns authentication back to the local controller:

```
default(config)# authentication-mode no-radius-profile
default(config)# authentication-mode local
```

Related Commands

- [radius-profile](#) on page 454
- [show authentication-mode](#) on page 478

authentication-mode global

Command Mode with authentication commands to configure administrators.

Syntax

`authentication-mode global`

Command Mode

Configuration Mode; this is another command mode under configuration.

Default

NA

Usage

Once you enter **configure terminal** then **authentication-mode global**, the (config-auth-mode) is added to the prompt and you can use the [authentication-type on page 384](#) commands.

Examples

The following sets both primary and secondary authentication mode to Radius, and provides the Radius secret:

```
ramcntrl(0)# configure terminal
ramcntrl(0)(config)# authentication-mode global
ramcntrl(0)(config-auth-mode)# authentication-type radius
ramcntrl(0)(config-auth-mode)# primary-radius-ip 172.18.1.3
ramcntrl(0)(config-auth-mode)# primary-radius-secret RadiusP
ramcntrl(0)(config-auth-mode)# secondary-radius-ip 172.18.1.7
ramcntrl(0)(config-auth-mode)# secondary-radius-secret RadiusS
ramcntrl(0)(config-auth-mode)# exit
ramcntrl(0)(config)# exit
ramcntrl(0)# sh authentication-mode
Administrative User Management
AuthenticationType : radius
Primary RADIUS IP Address : 172.18.1.3
Primary RADIUS Port : 1812
Primary RADIUS Secret Key : *****
Secondary RADIUS IP Address : 172.18.1.7
Secondary RADIUS Port : 1812
Secondary RADIUS Secret Key : *****
```

```
Primary TACACS+ IP Address : 0.0.0.0
Primary TACACS+ Port : 49
Primary TACACS+ Secret Key : *****
Secondary TACACS+ IP Address : 0.0.0.0
Secondary TACACS+ Port : 49
Secondary TACACS+ Secret Key : *****
ramcntrl(0)#
```

Related Commands

- [authentication-type](#) on page 384
- [show authentication-mode](#) on page 478

authentication-type

Sets the authentication type (in authentication mode) for controller user login.

Syntax

```
authentication-type local
authentication-type radius
authentication-type primary-radius <profile_name>
authentication-type secondary-radius <profile_name>
authentication-type no-primary-radius
authentication-type no-secondary-radius}
```

local (default)	The local controller performs the user authentication. If authentication type is local, only local guest users will be valid. Session-timeout and Activity time out controller values are used. Local is the default, and if that fails, Radius authentication is checked.
radius	A Radius server performs the user authentication. Only Radius server users will be valid. Session-timeout and Activity time out Radius servervalues are used. Also if the Session timeout value is not configured in the Radius server, then the controller session timeout value will be used. If Radius fails, local authentication is not checked.
primary-radius	Specifies the name of the primary Radius server profile.
secondary-radius	Specifies the name of the secondary Radius server profile.
profile_name	The profile name of the primary or secondary Radius server.
no-primary-radius	Disables the primary Radius server from performing authentication.
no-secondary-radius	Disables the secondary Radius server from performing authentication.

Command Mode

Configuration mode

Default

none

Usage

Use this command to determine where authentication for Web users occurs. Authentication can be performed by the controller locally (using the **local** argument) or by a primary and secondary RADIUS server (using the **radius** argument) or by both (**local and radius**).

If the **radius** option is used, the name of the primary and optionally, the secondary, Radius server (specified in the *profile_name* argument) is used. The profile name for these servers must already have been created with the **radius-profile** command.

If the **radius** option is specified, a user name and password with the controller's IP address must be created on the external RADIUS server for each userid to be authenticated.

Use **no-primary-radius** or **no-secondary-radius** arguments to disable the RADIUS server authentication configuration.

Examples

The following commands set local controller authentication:

```
default(config)# authentication-mode local
```

The following commands enable the primary Radius server configured in the Primary profile name to perform user authentication:

```
default(config)# authentication-mode radius
default(config)# authentication-mode radius-profile
default(config)# authentication-mode primary-radius Primary
```

The following commands disables the primary Radius server from performing user authentication and returns authentication back to the local controller:

```
default(config)# authentication-mode no-radius-profile
default(config)# authentication-mode local
```

The following sets both primary and secondary authentication mode to Radius, and provides the Radius secret:

```
ramcntrl(0)# configure terminal
ramcntrl(0)(config)# authentication-mode global
ramcntrl(0)(config-auth-mode)# authentication-type radius
ramcntrl(0)(config-auth-mode)# primary-radiusprimary-
radius-ip primary-radius-port primary-radius-secret
ramcntrl(0)(config-auth-mode)# primary-radius-ip 172.18.1.3
ramcntrl(0)(config-auth-mode)# primary-radius-secret RadiusP
ramcntrl(0)(config-auth-mode)# secondary-radiussecondary-
radius-ip secondary-radius-port secondary-radius-secret
8
(6-8)
```

Operator is the lowest authentication level and also the default. Operators

can see statistics and results but cannot make any configuration changes.

5

(3-5)

Administrators can also do general configuration changes, but cannot upgrade APs or controllers, nor can they upgrade FortiWLC (SD) versions using

Telnet. They cannot configure an NMS server, NTP server, change the system password, date or time (all CLI). They cannot create local admins, a new feature in release 4.1, nor can they set the authentication mode for a controller (GUI and CLI). Administrators cannot add or remove licensing.

2

(0-2)

SuperUser administrators can perform all configurations on the controller.

They are the only ones who can upgrade APs or controllers and they can upgrade FortiWLC (SD) versions using Telnet. They can configure an NMS server, NTP server, system password, date and time (all CLI). They can also create other admins and set the authentication mode for a controller (GUI and

CLI). Superusers can add and remove licensing.

Radius Authentication

© 2015 Fortinet, Inc. Authentication 141

4.1 Beta

```
ramcntrl(0)(config-auth-mode)# secondary-radius-ip 172.18.1.7
```

```
ramcntrl(0)(config-auth-mode)# secondary-radius-secret RadiusS
```

```
ramcntrl(0)(config-auth-mode)# exit
```

```
ramcntrl(0)(config)# exit
```

```
ramcntrl(0)# sh authentication-mode
```

Administrative User Management

AuthenticationType : radius

Primary RADIUS IP Address : 172.18.1.3

Primary RADIUS Port : 1812

Primary RADIUS Secret Key : *****

Secondary RADIUS IP Address : 172.18.1.7

Secondary RADIUS Port : 1812

Secondary RADIUS Secret Key : *****

Primary TACACS+ IP Address : 0.0.0.0
Primary TACACS+ Port : 49
Primary TACACS+ Secret Key : *****
Secondary TACACS+ IP Address : 0.0.0.0
Secondary TACACS+ Port : 49
Secondary TACACS+ Secret Key : *****
ramcntrl(0)#

Related Commands

- [radius-profile](#) on page 454
- [show authentication-mode](#) on page 478

captive-portal

Enables the captive portal feature.

Syntax

```
captive-portal disabled  
captive-portal webauth  
no captive-portal
```

<code>disabled</code>	Disables the Captive Portal feature.
<code>webauth</code>	Enables WebAuth for the Captive Portal.

Command Mode

Security profile configuration

Default

Captive portal is disabled.

Usage

Use this command to enable the Captive Portal Webauth in a security profile. If captive portal is enabled, a station attempting to associate to the ESS is directed to a WebAuth login page (the Captive Portal).

If Captive Portal is enabled for Webauth, the HTTPS protocol and Secure Socket Layer (SSL) provide an encrypted login interchange until the client station authentication and authorization is completed. A RADIUS authentication server is used as a backend to determine user access. All traffic from the client except DHCP, ARP, and DNS packets are dropped until access is granted. If access is not granted, the station is unable to leave the Captive Portal. If access is granted, the user is released from the Captive Portal and can enter the WLAN.

Use **no captive-portal** or **captive-portal disabled** to disable the captive portal feature.

Examples

The following commands enable a WebAuth captive portal for the Security Profile:

```
default# configure terminal  
default(config)# security-profile web_auth  
default(config-security)# captive-portal webauth  
default(config-security)# radius-server primary main-auth  
default(config-security)# exit
```



```
default(config)# exit
```

Related Commands

- [*radius-server primary*](#) **on page 456**
- [*ssl-server radius-profile*](#) **on page 498**
- [*captive-portal-auth-method*](#) **on page 390**

captive-portal-auth-method

Sets authentication to internal (default) for Fortinet or external for third-party solutions.

Syntax `captive-portal-auth-method internal`
 `captive-portal-auth-method external`

Command Mode Configuration Mode, Security Mode

Default Fortinet Captive Portal

Usage Instead of using the Fortinet Captive Portal solution, you can use a third-party solution; you cannot use both. Companies such as Bradford, Avenda, and CloudPath all provide Captive Portal solutions that work with FortiWLC (SD) 4.1 and later. There are two places that you need to indicate a third-party captive portal solution, in the corresponding Security Profile and in the Captive Portal configuration. Indicate that a third-party Captive Portal solution will be used in the Security Profile with the CLI command **captive-portal-auth-method**. Indicate that a third-party Captive Portal solution will be used in the Captive Portal configuration with the CLI command **ssl-server captive-portal-external-URL**. Then, provide the URL for the Captive Portal box with the command **change_mac_state**.

Examples This example configures third-party Captive Portal with the CLI by completing these two tasks:

Indicate that a third-party Captive Portal solution will be used in the Security Profile with the CLI command **captive-portal-auth-method**. For example:

```
controller1# configure terminal
controller1(config)# security-profile CPExternal
controller1(config-security)# captive-portal-auth-method
external internal
controller1(config-security)# captive-portal-auth-method ?
<captivePortAuthMethod> Configure captive portal authentication method.
external external
internal internal
controller1(config-security)# captive-portal-auth-method external
```

Indicate that a third-party Captive Portal solution will be used in the Captive Portal configuration with the CLI command **ssl-server captive-portal-external-URL**. Then, provide the URL for the Captive Portal box with the command **change_mac_state**. For example:

```
controller1# configure terminal
controller1(config)# ssl-server ca
captive-portal captive-portal-external-URL
controller1(config)# ssl-server captive-portal-external-URL
controller1(config)# exit
controller1# change_mac_state ?
<ip-address> Enter the Client IP Address.
controller1# change_mac_state 172.18.19.14 ?
off Web Auth mode off.
on Web Auth mode on.
controller1# change_mac_state 172.18.19.14 on ?
<CR>
<filter-id> Enter the Filter Id.
controller1# change_mac_state 172.18.19.14 on ftp_only
Configure a Radius Server for Captive Portal Authentication
© 2010 Fortinet, Inc. Captive Portals for Temporary Users 169
4.1 Beta
<CR>
controller1# change_mac_state 172.18.19.14 on ftp_only
controller1#
controller1# change_mac_state 172.18.19.14 ?
off Web Auth mode off.
on Web Auth mode on.
controller1# change_mac_state 172.18.19.14 off ?
<CR>
<filter-id> Enter the Filter Id.
controller1# change_mac_state 172.18.19.14 off
controller1
```

Related Commands

[change_mac_state](#) on page 416

cef

Configures the Common Event Format Logging feature.

Syntax

```
cef server-ip<hostname> <port>
cef server-ip<IP address> <port>
cef server-ip<hostname>
cef server-ip<IP address>
cef enable
cef disable
```

hostname	The IP address or hostname of the remote server.
ip address	
port	The server port for use. By default, 514 is used.

Command Mode

Global configuration

Default

Disabled is default.

Usage

Use this command to translate syslog messages into Common Event Format logging to support interoperability with ArcSight logging servers, in addition to the standard syslog format.

Before enabling this feature, configure the hostname or IP address of the ArcSight server where logging is performed.

The following show some events that trigger syslog messages, and the information contained with the message:

Event that triggers a syslog message	Information available in the syslog message
Wireless associations	MAC Address, SSID, AP number, BSSID and timestamp
1x Authentication Attempt	Username, MAC address and AP number
1x Authentication failure	Username, MAC address and AP number

Event that triggers a syslog message	Information available in the syslog message
For Qos and firewall rules configured to be logged, the action taken on the network traffic whether permitted or denied.	MAC address, IP address and AP MAC address
All access to the controller management interface	Timestamp, IP address
Rogue AP detection	Rogue BSSID, AP number
Controller Up	Timestamp
AP Down	AP number, Timestamp
AP Up	AP number, Timestamp
Controller State Transition (Master ? Slave)	

The following are the Device Class Event IDs:

No	Event	DeviceEventClassId
1	Wireless associations	Wireless Associations
2	1x Authentication Attempt	802.1x Authentication Attempt
3	1x Authentication failure	802.1x Authentication failure
4	For Qos and firewall rules configured to be logged, the action taken on the network traffic whether permitted or denied.	Network Traffic
5	All access to the controller management interface	Controller Access
6	Rogue AP detection	ROGUE AP DETECTED
7	Controller Up	Controller Up
8	AP Up	AP UP

No	Event	DeviceEventClassId
9	AP Down	AP DOWN
10	Controller State Transition (Master ? Slave)	Controller State Change
11	All other log messages	Common Fortinet Event

Examples

The following configures the cef logging server at 192.18.100.100 and enables cef:

```
default(config)# cef server-ip 192.168.100.100 255.255.255.0
default(config)# cef enable
```

This example lists CEF logging options and then shows the current CEF settings.

```
WiFi36# configure terminal
WiFi36(config)# cef ?
disable                Disables Common Event Format Logging Feature.
enable                 Enables Common Event Format Logging Feature.
server-ip              Enter Server Details
WiFi36(config)# exit
WiFi36#
WiFi36# show cef
CEF Logging is disabled
CEF Logging Host is not configured
WiFi36#
```

Related Commands

[show cef](#) on page 479

certmgmt delete-ca

Deletes a controller Trusted Root CA certificate.

Syntax

certmgmt delete-ca <cert-alias>

cert-alias The name of the certificate alias that was created with the Web UI.

Command Mode

Privileged EXEC

Default

NA

Usage

Use the **certmgmt delete-ca** command to delete a Trusted Root CA certificate from the controller's Certificates Repository.

The certificate can only be created and imported into the controller using the Web UI.

Trusted Root CA certificates are certificates of trusted third parties. Any client or server software that supports certificates maintains a collection of trusted Root CA certificates. These CA certificates determine which other certificates the software can validate. The software can validate only certificates issued by one of the CAs in the controller's Trusted Root CA Certificates Repository.

Examples

The following command deletes the Trusted Root CA certificate named ca1:

```
controller# certmgmt delete-ca ca1
controller#
```

Related Commands

- [*certmgmt delete-csr on page 397*](#)
- [*certmgmt delete-server on page 398*](#)
- [*certmgmt export-ca on page 400*](#)
- [*certmgmt export-csr on page 402*](#)
- [*certmgmt export-server on page 404*](#)
- [*certmgmt list-ca on page 406*](#)
- [*certmgmt list-csr on page 408*](#)
- [*certmgmt list-server on page 409*](#)

- [certmgmt view-ca](#) on page 411
- [certmgmt view-csr](#) on page 413
- [certmgmt view-server](#) on page 414
- [change_mac_state](#) on page 416

certmgmt delete-csr

Deletes a pending Certificate Signing Request (CSR).

Syntax

```
certmgmt delete-csr <cert-alias>
```

cert-alias The name of the certificate alias that was created with the Web UI.

Command Mode

Privileged EXEC

Default

NA

Usage

Use the **certmgmt delete-csr** command to delete a pending Certificate Signing Request (CSR) that was created with the Web UI. A pending CSR is the file that was sent to the CA for signing and for obtaining the signed certificate. Until the signed certificate is returned, the CSR status is considered pending.

Examples

The following command deletes the pending CSR for the certificate named ca1:

```
controller# certmgmt delete-csr ca1
controller#
```

Related Commands

- [certmgmt delete-ca on page 395](#)
- [certmgmt delete-server on page 398](#)
- [certmgmt export-ca on page 400](#)
- [certmgmt export-csr on page 402](#)
- [certmgmt export-server on page 404](#)
- [certmgmt list-ca on page 406](#)
- [certmgmt list-csr on page 408](#)
- [certmgmt list-server on page 409](#)
- [certmgmt view-ca on page 411](#)
- [certmgmt view-csr on page 413](#)
- [certmgmt view-server on page 414](#)
- [change_mac_state on page 416](#)

certmgmt delete-server

Deletes a controller Server Certificate.

Syntax

certmgmt delete-server <cert-alias>

cert-alias

The name of the certificate alias that was created with the Web UI.

Command Mode

Privileged EXEC

Default

NA

Usage

Use the **certmgmt delete-server** command to delete a Server Certificate from the controller's Certificates Repository. Note that you can delete Server Certificates with this CLI command but you can only create and import them into the controller from the Web UI.

Server Certificates are used by various applications for PKI purposes. The user of a Server Certificate initiates the process to create the private key and certificate request. This certificate request is sent to a CA/RA for signing. Once the CA has processed the certificate request, the certificate is then stored in the controller's Certificates Repository.

Examples

The following command deletes the Server Certificate named sc1:

```
controller# certmgmt delete-server sc1
controller#
```

Related Commands

- [*certmgmt delete-ca on page 395*](#)
- [*certmgmt delete-csr on page 397*](#)
- [*certmgmt export-ca on page 400*](#)
- [*certmgmt export-csr on page 402*](#)
- [*certmgmt export-server on page 404*](#)
- [*certmgmt list-ca on page 406*](#)
- [*certmgmt list-csr on page 408*](#)
- [*certmgmt list-server on page 409*](#)

- [certmgmt view-ca](#) on page 411
- [certmgmt view-csr](#) on page 413
- [certmgmt view-server](#) on page 414
- [change_mac_state](#) on page 416

certmgmt export-ca

Exports a pending controller Trusted Root CA certificate.

Syntax

certmgmt export-ca <cert-alias>

cert-alias The name of the certificate alias that was created with the Web UI.

Command Mode

Privileged EXEC

Default

NA

Usage

Use the **certmgmt export-ca** command to export a Trusted Root CA certificate from the controller's Certificates Repository to another location.

The certificate can only be created and imported into the controller using the Web UI.

Trusted Root CA certificates are certificates of trusted third parties. Any client or server software that supports certificates maintains a collection of trusted Root CA certificates. These CA certificates determine which other certificates the software can validate. The software can validate only certificates issued by one of the CAs in the controller's Trusted Root CA Certificates Repository. Note that you can export Server Certificates with this CLI command but you can only import them into the controller from the Web UI.

Examples

The following command exports the Trusted Root CA certificate named ca1:

```
controller# certmgmt export-ca ca1
controller#
```

Related Commands

- [certmgmt delete-ca on page 395](#)
- [certmgmt delete-csr on page 397](#)
- [certmgmt delete-server on page 398](#)
- [certmgmt export-csr on page 402](#)
- [certmgmt export-server on page 404](#)
- [certmgmt list-ca on page 406](#)

- [certmgmt list-csr](#) on page 408
- [certmgmt list-server](#) on page 409
- [certmgmt view-ca](#) on page 411
- [certmgmt view-csr](#) on page 413
- [certmgmt view-server](#) on page 414
- [change_mac_state](#) on page 416

certmgmt export-csr

Exports a pending Certificate Signing Request (CSR).

Syntax

certmgmt export-csr <cert-alias>

cert-alias The name of the certificate alias that was created with the Web UI.

Command Mode

Privileged EXEC

Default

NA

Usage

Use the **certmgmt export-csr** command to export a pending CSR to another location. The certificate can only be created and imported into the controller using the Web UI.

A pending CSR is the file that was sent to the CA for signing and for obtaining the signed certificate. Until the signed certificate is returned, the CSR status is considered pending.

Examples

The following command exports the CSR named ca1:

```
controller# certmgmt export-csr ca1
```

```
controller#
```

Related Commands

- [certmgmt delete-ca](#) on page 395
- [certmgmt delete-csr](#) on page 397
- [certmgmt delete-server](#) on page 398
- [certmgmt export-ca](#) on page 400
- [certmgmt export-server](#) on page 404
- [certmgmt list-ca](#) on page 406
- [certmgmt list-csr](#) on page 408
- [certmgmt list-server](#) on page 409
- [certmgmt view-ca](#) on page 411
- [certmgmt view-csr](#) on page 413

- [certmgmt view-server](#) **on page 414**
- [change_mac_state](#) **on page 416**

certmgmt export-server

Exports a controller Server Certificate.

Syntax

certmgmt export-server <cert-alias>

cert-alias The name of the certificate alias that was created with the Web UI.

Command Mode

Privileged EXEC

Default

NA

Usage

Use the **certmgmt export-server** command to export a Server Certificate from the controller's Certificates Repository to another location.

Server Certificates can only be created and imported into the controller using the Web UI.

Server Certificates are used by various applications for PKI purposes. The user of a Server Certificate initiates the process to create the private key and certificate request. This certificate request is sent to a CA/RA for signing. Once the CA has processed the certificate request, the certificate is then stored in the controller's Certificates Repository.

Examples

The following command exports the Server Certificate named sc1:

```
controller# certmgmt export-server sc1
controller#
```

Related Commands

- [*certmgmt delete-ca*](#) **on page 395**
- [*certmgmt delete-csr*](#) **on page 397**
- [*certmgmt delete-server*](#) **on page 398**
- [*certmgmt export-ca*](#) **on page 400**
- [*certmgmt export-csr*](#) **on page 402**
- [*certmgmt list-ca*](#) **on page 406**
- [*certmgmt list-csr*](#) **on page 408**
- [*certmgmt list-server*](#) **on page 409**

- [certmgmt view-ca](#) **on page 411**
- [certmgmt view-csr](#) **on page 413**
- [certmgmt view-server](#) **on page 414**
- [change_mac_state](#) **on page 416**

certmgmt list-ca

Lists a controller's Trusted Root CA certificates.

Syntax

certmgmt list-ca

Command Mode

Privileged EXEC

Default

NA

Usage

Use the **certmgmt list-ca** command to lists the Trusted Root CA certificates in the controller's Certificates Repository.

The certificate can only be created and imported into the controller using the Web UI.

Trusted Root CA certificates are certificates of trusted third parties. Any client or server software that supports certificates maintains a collection of trusted Root CA certificates. These CA certificates determine which other certificates the software can validate. The software can validate only certificates issued by one of the CAs in the controller's Trusted Root CA Certificates Repository.

Examples

The following command lists the Trusted Root CA certificate:

```
controller# certmgmt list-ca
```

```
Trusted Root CA Certificates
```

```
-----
```

Related Commands

- [certmgmt delete-ca on page 395](#)
- [certmgmt delete-csr on page 397](#)
- [certmgmt delete-server on page 398](#)
- [certmgmt export-ca on page 400](#)
- [certmgmt export-csr on page 402](#)
- [certmgmt export-server on page 404](#)
- [certmgmt list-csr on page 408](#)

- [certmgmt list-server](#) on page 409
- [certmgmt view-ca](#) on page 411
- [certmgmt view-csr](#) on page 413
- [certmgmt view-server](#) on page 414
- [change_mac_state](#) on page 416

certmgmt list-csr

Lists the pending Certificate Signing Request (CSR).

Syntax

certmgmt list-csr

Command Mode

Privileged EXEC

Default

NA

Usage

Use the **certmgmt list-csr** command to list the pending CSRs. Note that certificates can only be created and imported into the controller using the Web UI.

A pending CSR is the file that was sent to the CA for signing and for obtaining the signed certificate. Until the signed certificate is returned, the CSR status is considered pending.

Examples

The following command exports the CSR named ca1:

```
controller# certmgmt list-csr
Pending CSRs
-----
```

Related Commands

- [certmgmt delete-ca on page 395](#)
- [certmgmt delete-csr on page 397](#)
- [certmgmt delete-server on page 398](#)
- [certmgmt export-ca on page 400](#)
- [certmgmt export-csr on page 402](#)
- [certmgmt export-server on page 404](#)
- [certmgmt list-ca on page 406](#)
- [certmgmt list-server on page 409](#)
- [certmgmt view-ca on page 411](#)
- [certmgmt view-csr on page 413](#)
- [certmgmt view-server on page 414](#)
- [change_mac_state on page 416](#)

certmgmt list-server

Lists a controller's Server Certificates.

Syntax

certmgmt list-server

Command Mode

Privileged EXEC

Default

NA

Usage

Use the **certmgmt list-server** command to list a controller's Server Certificates (created and imported with the GUI) in the controller's Certificates Repository.

Server Certificates are used by various applications for PKI purposes. The user of a Server Certificate initiates the process to create the private key and certificate request. This certificate request is sent to a CA/RA for signing. Once the CA has processed the certificate request, the certificate is then stored in the controller's Certificates Repository.

Examples

The following command lists the controller's Server Certificates:

```
controller# certmgmt list-server
```

```
Server Certificates
-----
```

Related Commands

- [certmgmt delete-ca](#) on page 395
- [certmgmt delete-csr](#) on page 397
- [certmgmt delete-server](#) on page 398
- [certmgmt export-ca](#) on page 400
- [certmgmt export-csr](#) on page 402
- [certmgmt export-server](#) on page 404
- [certmgmt list-ca](#) on page 406
- [certmgmt list-csr](#) on page 408
- [certmgmt view-ca](#) on page 411
- [certmgmt view-csr](#) on page 413

- [certmgmt view-server](#) on page 414
- [change_mac_state](#) on page 416

certmgmt view-ca

Display a controller Trusted Root CA certificate.

Syntax

certmgmt view-ca <cert-alias>

cert-alias The name of the certificate alias that was created with the Web UI.

Command Mode

Privileged EXEC

Default

NA

Usage

Use the **certmgmt view-ca** command to view the details of a Trusted Root CA certificate. The certificate must first be created and imported into the controller using the Web UI.

Trusted Root CA certificates are certificates of trusted third parties. Any client or server software that supports certificates maintains a collection of trusted Root CA certificates. These CA certificates determine which other certificates the software can validate. The software can validate only certificates issued by one of the CAs in the controller's Trusted Root CA Certificates Repository.

Examples

The following command displays the Trusted Root CA certificate named ca1:

```
controller# certmgmt view-ca ca1
```

Related Commands

- [certmgmt delete-ca on page 395](#)
- [certmgmt delete-csr on page 397](#)
- [certmgmt delete-server on page 398](#)
- [certmgmt export-ca on page 400](#)
- [certmgmt export-csr on page 402](#)
- [certmgmt export-server on page 404](#)
- [certmgmt list-ca on page 406](#)
- [certmgmt list-csr on page 408](#)
- [certmgmt list-server on page 409](#)
- [certmgmt view-csr on page 413](#)

- [certmgmt view-server](#) **on page 414**
- [change_mac_state](#) **on page 416**

certmgmt view-csr

Display a pending Certificate Signing Request (CSR).

Syntax

```
certmgmt view-csr <cert-alias>
```

cert-alias The name of the certificate alias that was created with the Web UI.

Command Mode

Privileged EXEC

Default

NA

Usage

Use the **certmgmt view-csr** command to view details of a pending Certificate Signing Request (CSR) that was created with the Web UI. A pending CSR is the file that was sent to the CA for signing and for obtaining the signed certificate. Until the signed certificate is returned, the CSR status is considered pending.

Examples

The following command displays the pending CSR for the certificate named ca1:

```
controller# certmgmt view-csr ca1
controller#
```

Related Commands

- [certmgmt delete-ca on page 395](#)
- [certmgmt delete-csr on page 397](#)
- [certmgmt delete-server on page 398](#)
- [certmgmt export-ca on page 400](#)
- [certmgmt export-csr on page 402](#)
- [certmgmt export-server on page 404](#)
- [certmgmt list-ca on page 406](#)
- [certmgmt list-csr on page 408](#)
- [certmgmt list-server on page 409](#)
- [certmgmt view-ca on page 411](#)
- [certmgmt view-server on page 414](#)
- [change_mac_state on page 416](#)

certmgmt view-server

Displays a controller Server Certificate.

Syntax

certmgmt view-server <cert-alias>

cert-alias The name of the certificate alias that was created with the Web UI.

Command Mode

Privileged EXEC

Default

NA

Usage

Use the **certmgmt view-server** command to display a Server Certificate from the controller's Certificates Repository.

Server Certificates can only be created and imported into the controller using the Web UI.

Server Certificates are used by various applications for PKI purposes. The user of a Server Certificate initiates the process to create the private key and certificate request. This certificate request is sent to a CA/RA for signing. Once the CA has processed the certificate request, the certificate is then stored in the controller's Certificates Repository.

Examples

The following command displays the Server Certificate named sc1:

```
controller# certmgmt view-server sc1
controller#
```

Related Commands

- [*certmgmt delete-ca*](#) **on page 395**
- [*certmgmt delete-csr*](#) **on page 397**
- [*certmgmt delete-server*](#) **on page 398**
- [*certmgmt export-ca*](#) **on page 400**
- [*certmgmt export-csr*](#) **on page 402**
- [*certmgmt export-server*](#) **on page 404**
- [*certmgmt list-ca*](#) **on page 406**
- [*certmgmt list-csr*](#) **on page 408**

- [certmgmt list-server](#) on page 409
- [certmgmt view-ca](#) on page 411
- [certmgmt view-csr](#) on page 413
- [change_mac_state](#) on page 416

change_mac_state

Works with captive-portal-auth-method to indicate the URL of the third-party Captive Portal solution.

Syntax

```
change_mac_state <IP address> on <filter ID>
change_mac_state <IP address> off
```

Command Mode

Configuration Mode, Security Mode

Default

Fortinet Captive Portal

Usage

Instead of using the Fortinet Captive Portal solution, you can use a third-party solution; you cannot use both. Companies such as Bradford, Avenda, and CloudPath all provide Captive Portal solutions that work with FortiWLC (SD) 4.1 and later. There are two places that you need to indicate a third-party captive portal solution, in the corresponding Security Profile and in the Captive Portal configuration. Indicate that a third-party Captive Portal solution will be used in the Security Profile with the CLI command **captive-portal-auth-method**. Indicate that a third-party Captive Portal solution will be used in the Captive Portal configuration with the CLI command **ssl-server captive-portal-external-URL**. Then, provide the URL for the Captive Portal box with the command **change_mac_state**.

Examples

This example configures third-party Captive Portal with the CLI by completing these two tasks:

Indicate that a third-party Captive Portal solution will be used in the Security Profile with the CLI command **captive-portal-auth-method**. For example:

```
controller1# configure terminal
controller1(config)# security-profile CPExternal
controller1(config-security)# captive-portal-auth-method
external internal
controller1(config-security)# captive-portal-auth-method ?
<captivePortAuthMethod> Configure captive portal authentication method.
external external
internal internal
controller1(config-security)# captive-portal-auth-method external
```

Indicate that a third-party Captive Portal solution will be used in the Captive Portal configuration with the CLI command **ssl-server captive-portal-external-URL**. Then, provide the URL for the Captive Portal box with the command **change_mac_state**. For example:

```
controller1# configure terminal
controller1(config)# ssl-server ca
captive-portal captive-portal-external-URL
controller1(config)# ssl-server captive-portal-external-URL
controller1(config)# exit
controller1# change_mac_state ?
<ip-address> Enter the Client IP Address.
controller1# change_mac_state 172.18.19.14 ?
off Web Auth mode off.
on Web Auth mode on.
controller1# change_mac_state 172.18.19.14 on ?
<CR>
<filter-id> Enter the Filter Id.
controller1# change_mac_state 172.18.19.14 on ftp_only
Configure a Radius Server for Captive Portal Authentication
© 2010 Fortinet, Inc. Captive Portals for Temporary Users 169
4.1 Beta
<CR>
controller1# change_mac_state 172.18.19.14 on ftp_only
controller1#
controller1# change_mac_state 172.18.19.14 ?
off Web Auth mode off.
on Web Auth mode on.
controller1# change_mac_state 172.18.19.14 off ?
<CR>
<filter-id> Enter the Filter Id.
controller1# change_mac_state 172.18.19.14 off
controller1
```

Related Commands

[captive-portal-auth-method](#) on page 390

clear certificates

Deletes the unassigned PEM and PFX certificate files.

Syntax

clear certificates

Command Mode

Privileged EXEC

Default

NA

Usage

Use the **clear certificates** command to remove unused .pem and .pfx certificate files. These are certificate files that have been imported into the system using the Web UI, but are not assigned to an application.

Examples

This command clears all unused certificates:

```
controller# clear certificates
```

Related Commands

[certmgmt delete-server](#) **on page 398**

description

Provides a description of the RADIUS profile server.

Syntax

description <text>

text Describes the RADIUS profile server. The text string can be a maximum of 128 characters and must be enclosed within double quotes.

Command Mode

RADIUS profile configuration

Default

NA

Usage

Use this command to provide descriptive information about the RADIUS profile. Enclose the descriptive text within double quotation marks. A maximum of 128 characters can be used. View the description using the detailed **show radius-profile** command, that is, using the profile argument.

Examples

```
controller(config-radius)# description
"This server is located on the Second floor of building G in the NW server
area."

controller(config-radius)# do show radius-profile RAD1
RADIUS Profile Table
RADIUS Profile Name      :RAD1
Description               :This server is located on the Second floor of
building G in the NW server area.
RADIUS IP                 :192.168.100.1
RADIUS Secret             :*****
RADIUS Port               :1812
RADIUS VLAN Name         :
MAC Address Delimiter     :none
Password Type             : shared-secret
```

Related Commands

- [radius-profile on page 454](#)
- [show radius-profile on page 482](#)

encryption-modes ccmp

Configures CCMP as the security profile cipher suite.

Syntax

```
encryption-modes ccmp  
no encryption-modes ccmp
```

Command Mode

Security Profile configuration

Default

No cipher is configured.

Usage

Use this command to set the cipher suite for a WPA2 security profile to CCMP, the encryption standard that is used with a WPA2 configuration.

Examples

The following command sets the encryption mode to CCMP:

```
controller(config-security)# encryption-modes ccmp  
controller(config-security)#
```

Related Commands

- [802.1x-network-initiation](#) on page 361
- [radius-profile](#) on page 454

encryption-modes ccmp-tkip

Configures CCMP and TKIP as the security profile cipher suite.

Syntax

```
encryption-modes ccmp-tkip  
no encryption-modes ccmp-tkip
```

Command Mode

Security Profile configuration

Default

No cipher is configured.

Usage

Use this command to set the cipher suite for WPA and WPA2 compatibility in the security profile by configuring both CCMP and TKIP for encryption.

Examples

The following command sets the encryption mode to CCMP/TKIP:

```
controller(config-security)# encryption-modes ccmp-tkip  
controller(config-security)#
```

Related Commands

- [802.1x-network-initiation](#) on page 361
- [encryption-modes ccmp](#) on page 420
- [encryption-modes tkip](#) on page 422
- [radius-profile](#) on page 454

encryption-modes tkip

Configures TKIP as the security profile cipher suite.

Syntax

```
encryption-modes tkip  
no encryption-modes tkip
```

Command Mode

Security Profile configuration

Default

No cipher is configured.

Usage

Use this command to set the cipher suite for the security profile to Temporal Key Integrity Check (TKIP). As part of the Wi-Fi Protection Access (WPA) solution to address the weaknesses in WEP, TKIP expands the size of the encryption key, increases the number of keys in use, and creates a message integrity checking mechanism. The other part of the WPA solution that should be implemented to ensure increased over-the-air data protection is the access control and key rotation provided by 802.1X, using one of the standard Extensible Authentication Protocol types (see **radius-profile** for 802.1X setup).

TKIP is a Layer 2 encryption algorithm that uses a 128-bit key and a 64-bit Initialization Vector (IV). TKIP uses the RC4 algorithm along with a symmetrical key to produce encrypted text. The symmetrical key is used for encrypting and decrypting text, and can be automatically distributed to an AP or user station when the 802.1X EAP solution is also implemented. TKIP uses the Message Integrity Check (MIC) to make sure the content of the data packets have not been changed during packet transmission.

Examples

The following command sets the encryption mode to TKIP:

```
controller(config-security)# encryption-modes tkip  
controller(config-security)#
```

Related Commands

- [802.1x-network-initiation](#) on page 361
- [radius-profile](#) on page 454

encryption-modes wep128

Configures WEP-128 as the security profile cipher suite.

Syntax

```
encryption-modes wep128  
no encryption-modes wep128
```

Command Mode

Security Profile configuration

Default

No cipher suite is configured.

Usage

Use this command to set the cipher suite for the security profile to WEP-128, also known as WEP2. WEP-128 is a Layer 2 encryption algorithm that uses a 104-bit key and a 24-bit Initialization Vector (IV). WEP2 uses the RC4 algorithm along with a symmetrical key to produce encrypted text. The symmetrical key is used for encrypting and decrypting text, and is manually distributed to an AP or user station, as opposed to being automatically generated. The key is in use until it is changed by the administrator. Alternately, you can configure the security profile to also use the 802.1X protocol to automatically generate the key, producing “Dynamic WEP,” a more secure form of WEP.

Examples

The following command sets the encryption mode to WEP-128:

```
controller(config-security)# encryption-modes wep128  
controller(config-security)#
```

Related Commands

- [8021x-network-initiation](#) on page 361
- [allowed-l2-modes](#) on page 373
- [encryption-modes wep64](#) on page 424
- [rekey period](#) on page 459
- [static-wep key](#) on page 501

encryption-modes wep64

Configures WEP-64 as the security profile cipher suite.

Syntax

```
encryption-modes wep64
no encryption-modes wep64
```

Command Mode

Security Profile configuration

Default

No cipher suite is configured.

Command Mode

Use this command to set the cipher suite for the security profile to WEP-64, a weaker form of encryption than WEP-128. WEP-64 (also known as WEP or WEP40) is a Layer 2 encryption algorithm that uses a 40-bit key and a 24-bit Initialization Vector (IV). WEP uses the RC4 algorithm along with a symmetrical key to produce encrypted text. The symmetrical key is used for encrypting and decrypting text, and is manually distributed to an AP or user station, as opposed to being automatically generated. The key is in use until it is changed by the administrator. Alternately, you can configure the security profile to also use the 802.1X protocol to automatically generate the key, producing “Dynamic WEP,” a more secure form of WEP.

Examples

The following command sets the encryption mode to WEP-64:

```
controller(config-security)# encryption-modes wep64
controller(config-security)#
```

Related Commands

- [802.1x-network-initiation](#) on page 361
- [allowed-l2-modes](#) on page 373
- [encryption-modes wep128](#) on page 423
- [rekey period](#) on page 459
- [static-wep key](#) on page 501

firewall-capability

Selects the configuration source for per-user firewall.

Syntax

```
firewall-capability configured
firewall-capability none
firewall-capability radius-configured
```

Command Mode

Security profile configuration

Default

Firewall capability is set to **none**.

Usage

Per-user firewall restricts network usage on a per-user basis by dropping or allowing traffic based on configured policies applied on a firewall tag associated with the user. Per-user firewall support is implemented either on the basis of the RADIUS-returned *filter-id* attribute, or a configured *firewall filter-id* parameter as part of the ESS profile configuration.

In the case of RADIUS-based per-user firewall support, the returned filter-id attribute, as part of the Access-Accept message, is used as the firewall tag and action is taken by applying configured firewall policies on this firewall tag.

In absence of RADIUS configuration, a configured firewall tag in the ESS profile can be used for defining the action by applying configured firewall policies. In this case, all users connecting to a given ESS profile are allocated the same firewall tag as the one configured for the profile.

Examples

The following command sets the firewall configuration to the RADIUS server values:

```
forti-wifi # configure terminal
forti-wifi (config)# security-profile web_auth
forti-wifi(config-security)# firewall-capability radius-configured
```

Related Commands

- [firewall-filter-id](#) on page 426
- [show security-profile](#) on page 484

firewall-filter-id

This command also applies to Quality of Service Commands and is explained in that chapter. See [firewall-filter-id](#) **on page 702**.

firewall-filter-id-flow

This command also applies to Quality of Service Commands and is explained in that chapter. See [firewall-filter-id-flow](#) on **page 704**.

group-rekey interval

Configures the wpa/802.1x profiles only with key rotation enabled

Syntax

```
group-rekey interval <n>  
no group-rekey interval
```

n .Number of seconds between retries. The range is 0-65535.

Command Mode

Security profile configuration

Default

Zero is set as the default.

Usage

Configures the wpa/802.1x profiles (only with key rotation enabled) in seconds.

To disable, use the **no** form of the command.

Example

This example configures group-rekey interval as 120 for a WPA profile:

```
rao36vcell# configure terminal  
rao36vcell(config)# security-profile kddi  
rao36vcell(config-security)# allowed-l2-modes wpa  
rao36vcell(config-security)# encryption-modes tkip  
rao36vcell(config-security)# radius-server primary IAS  
rao36vcell(config-security)# key-rotation enabled  
rao36vcell(config-security)# group-rekey interval 120  
rao36vcell(config-security)# exit  
rao36vcell(config)# exit
```

Related Commands

- [security-profile](#) on page 467
- [802.1x-network-initiation](#) on page 361
- [allowed-l2-modes](#) on page 373
- [encryption-modes tkip](#) on page 422
- [psk key](#) on page 452
- [show security-profile](#) on page 484

import

This command is obsolete and has been blocked in 4.0 release. It used to import a security certificate from remote site via SCP. Please use the GUI to import and manage certificates.

ip-address

Sets the IP address for the profiled RADIUS server.

Syntax

ip-address <address>

address The IP address of the profiled RADIUS server.

Command Mode

RADIUS server profile configuration mode.

Default

NA

Usage

This command sets the IP address of the server being configured for the RADIUS profile. The RADIUS server is a key component of 802.1X WLAN security, as it provides access management by checking an access list to authenticate a user that attempts to join the WLAN.

Many sites configure a primary and secondary RADIUS server to ensure the continued availability of the authentication service, should the primary server become unavailable.

A RADIUS server IP address and passkey are required for configuration.

After the profile for the RADIUS server is configured, use the **radius-server primary** and **radius-server secondary** commands from within the Security Profile to enable the authentication service.

Examples

```
controller(config-radius)# ip-address 10.2.2.2
```

Related Commands

- [*key on page 431*](#)
- [*mac-delimiter on page 435*](#)
- [*radius-profile on page 454*](#)
- [*port on page 442*](#)
- [*radius-server primary on page 456*](#)
- [*radius-server secondary on page 457*](#)
- [*show radius-profile on page 482*](#)

key

Configure the profiled RADIUS server secret key.

Syntax

key <*secret*>
no key

secret Specifies the secret key used by the RADIUS server. A maximum of 64 characters is permitted (the ! character cannot be used).

Command Mode

RADIUS server profile configuration mode.

Default

No key is assigned.

Usage

Use this command to set the secret key for the RADIUS server being configured in the RADIUS server profile.

Examples

The following command sets the key for the profiled RADIUS server to **mysecret**:

```
controller(config-radius)# key mysecret  
controller(config-radius)#
```

Related Commands

[*radius-profile*](#) on page 454

key-rotation

Configure the key rotation behavior.

Syntax

`key-rotation enabled`
`key-rotation disabled`

Command Mode

Security profile configuration mode

Default

NA

Usage

Use this command to set the rotation for the secret key.

Examples

The following command enables key rotation:

```
controller(config-security)# key-rotation enabled
```

local-admin

Configures administrators for local mode authentication and enters local admin configuration mode where you can specify [password on page 437](#) and [privilege-level on page 449](#) for the named local admin.

Syntax

`local-admin <name>`

Command Mode

Configuration Mode; Local Admin is also a mode where you set the password and privilege level for the admin.

Default

NA

Usage

Use these commands, new in release 4.1, to configure local administrators:

- [authentication-mode global on page 382](#)
- [authentication-type on page 384](#) local
- local-admin (this command)
- password (only works in local-admin mode)
- privilege-level (only works in local-admin mode)
- [show local-admins on page 480](#)

Examples

The following configures a local admin:

```
ramcntrl(0)# configure terminal
ramcntrl(0)(config)# authentication-mode global
ramcntrl(0)(config-auth-mode)# authentication-type local
ramcntrl(0)(config-auth-mode)# exit
ramcntrl(0)(config)# exit
ramcntrl(0)# sh authentication-mode
Administrative User Management
AuthenticationType : local
Primary RADIUS IP Address : 0.0.0.0
Primary RADIUS Port : 1812
Primary RADIUS Secret Key : *****
Secondary RADIUS IP Address : 0.0.0.0
```

```
Secondary RADIUS Port : 1812
Secondary RADIUS Secret Key : *****
Primary TACACS+ IP Address : 0.0.0.0
Primary TACACS+ Port : 49
Primary TACACS+ Secret Key : *****
Secondary TACACS+ IP Address : 0.0.0.0
Secondary TACACS+ Port : 49
Secondary TACACS+ Secret Key : *****
ramcntrl(0)#
ramcntrl(0)(config)# local-admin JCalhoun
ramcntrl(0)(config-local-admin)# privilege-level 2
ramcntrl(0)(config-local-admin)# password yosemite44
ramcntrl(0)(config-local-admin)# exit
ramcntrl(0)(config)# exit
```

Related Commands

- [password](#) on page 437
- [privilege-level](#) on page 449
- [show local-admins](#) on page 480

mac-delimiter

Sets the delimiter character for the RADIUS server profile.

Syntax

```
mac-delimiter colon
mac-delimiter hyphen
mac-delimiter none
mac-delimiter single hyphen
no mac-delimiter
```

colon	Specifies the delimiter to the colon character (:).
hyphen	Specifies the delimiter to the hyphen character (-).
singlehyphen	Specifies the delimiter as a single hyphen character (-) between each of 3 octets (e.g. abcdef-abcdef).
none	Specifies that no delimiter is to be used (default).

Command Mode

RADIUS server profile configuration mode.

Default

No delimiter is assigned.

Usage

This command sets the delimiter character for the RADIUS server profile. It specifies the delimiter that is used on the RADIUS server to separate records within the server database.

Examples

```
controller(config-radius)# mac-delimiter colon
```

Related Commands

- [radius-profile on page 454](#)
- [ip-address on page 430](#)
- [key on page 431](#)
- [port on page 442](#)
- [radius-server primary on page 456](#)
- [radius-server secondary on page 457](#)

macfiltering

Enables MAC filtering for a security profile.

Syntax

macfiltering
no macfiltering

Command Mode

Security Profile configuration

Default

MAC filtering is disabled.

Usage

This command allow you to enable and disable MAC filtering specifically for a Security Profile. The command is useful to override the global MAC filtering setting for an ESS by using the **no macfiltering** command from within the Security Profile.

Examples

The following command disables MAC filtering for the Security Profile.

```
controller(config-security)# no macfiltering
```

Related Commands

[access-list permit](#) on page 367

password

Configures local mode authentication password for an admin.

Syntax

password <passwd>

Command Mode

Configuration Mode > Local Admin Mode

Default

NA

Usage

Use these commands, new in release 4.1, to configure local administrators:

- [authentication-mode global on page 382](#)
- [authentication-type on page 384](#)
- [local-admin on page 433](#)
- password (only works in local-admin mode)
- privilege-level (only works in local-admin mode)
- [show local-admins on page 480](#)

Examples

The following configures a local admin:

```
ramcntrl(0)# configure terminal
ramcntrl(0)(config)# authentication-mode global
ramcntrl(0)(config-auth-mode)# authentication-type local
ramcntrl(0)(config-auth-mode)# exit
ramcntrl(0)(config)# exit
ramcntrl(0)# sh authentication-mode
Administrative User Management
AuthenticationType : local
Primary RADIUS IP Address : 0.0.0.0
Primary RADIUS Port : 1812
Primary RADIUS Secret Key : *****
Secondary RADIUS IP Address : 0.0.0.0
Secondary RADIUS Port : 1812
```

```
Secondary RADIUS Secret Key : *****
Primary TACACS+ IP Address : 0.0.0.0
Primary TACACS+ Port : 49
Primary TACACS+ Secret Key : *****
Secondary TACACS+ IP Address : 0.0.0.0
Secondary TACACS+ Port : 49
Secondary TACACS+ Secret Key : *****
ramcntrl(0)#
ramcntrl(0)(config)# local-admin JCalhoun
ramcntrl(0)(config-local-admin)# privilege-level 2
ramcntrl(0)(config-local-admin)# password yosemite44
ramcntrl(0)(config-local-admin)# exit
ramcntrl(0)(config)# exit
```

Related Commands

- [local-admin](#) on page 433
- [privilege-level](#) on page 449

password-type

Configure the profiled RADIUS server password type.

Syntax

```
password-type shared-secret  
password-type mac-address  
no password-type
```

shared-secret	Specifies that the secret key in use by the RADIUS server is used for passwords. The key command must be configured.
mac-address	Sets the password to the MAC address of a client, as set in the RADIUS for MAC filtering configuration.

Command Mode

RADIUS server profile configuration mode.

Default

The shared-secret is set.

Usage

Use this command to set the type of password that is to be used for client access. By default, the secret key for the RADIUS server that is configured with the key command in the RADIUS server profile is used. If the mac-address type is selected, the MAC address of a client is used as the password for clients set as users in RADIUS for MAC filtering.

Examples

The following command sets the password type to mac-address for the profiled RADIUS server:

```
controller(config-radius)# password-type mac-address  
controller(config-radius)#
```

Related Commands

[radius-profile](#) on page 454

PMK-caching

Enables PMK caching for the selected security profile. Note that this function only applies to WPA2 and Mixed security profiles.

Syntax

```
pmk-caching  
no pmk-caching
```

Command Mode

Security Profile configuration

Default

By default, PMK caching is enabled.

Usage

This command enables or disables the use of Pairwise Master Key (PMK) caching on the active security profile. PMK caching allows wireless clients and APs to cache authentication results, allowing faster network access when a client is roaming back to an AP to which it had already authenticated previously.

Use the **no pmk-caching** command to disable pmk-caching.

Examples

The following command changes the key every 300 seconds (5 minutes):

```
MC3200-5072(15)# configure terminal  
MC3200-5072(15)(config)# security-profile Wpa2Test  
MC3200-5072(15)(config-security)# pmk-caching  
MC3200-5072(15)(config-security)# end
```

Related Commands

pmk caching

This command enables and disables PMK caching for KDDI phones.

Syntax

`pmk caching [enabled | disabled]`

Command Mode

Security profile configuration

Default

This option is only available when WPA is chosen for L2 encryption.

Usage

From the Security Profile configuration, enable or disable PMK caching for KDDI phones. The system automatically detects the KDDI phone using the KDDI Vendor ID and applies PMK caching if available.

Examples

To enable PMK caching, add the following line to the WPA security profile configuration:

```
default(config-security)# pmk caching enabled
```

To disable PMK caching, execute the following command at the WPA security profile configuration:

```
default(config-security)# pmk caching disabled
```

Related Commands

- [security-profile](#) on page 467
- [radius-server primary](#) on page 456
- [radius-server secondary](#) on page 457
- [802.1x-network-initiation](#) on page 361
- [show security-profile](#) on page 484

port

Sets the port number for the RADIUS server profile.

Syntax

```
port port  
no port
```

port	Specifies the port to be used in the RADIUS Authentication server profile. Valid port numbers are from 1024 to 65535. By default, port 1812 is set. Port 1813 should be used for an Accounting RADIUS server.
------	---

Command Mode

RADIUS server profile configuration mode.

Default

Port 1812 is assigned.

Usage

This command sets the port used for the RADIUS server profile. Usually this setting does not need to be changed unless the profile is used for a RADIUS accounting server, in which case it should be changed to 1813.

Examples

```
controller# config terminal  
controller(config)#  
controller(config-radius)# port 6600
```

Related Commands

- [ip-address](#) on page 430
- [key](#) on page 431
- [radius-server primary](#) on page 456
- [radius-server secondary](#) on page 457
- [radius-profile](#) on page 454
- [port](#) on page 442
- [show radius-profile](#) on page 482

primary-tacacs-ip

Designates the IP address of the primary TACACS+ server.

Syntax

primary-tacacs-ip <xx.xx.xx.xx>

Command Mode

Configuration Mode > Authentication Mode

Default

NA

Usage

New commands to configure TACACS+ authentication mode for all administrators on a Cisco ACS server were introduced in FortiWLC (SD) 4.1:

- [authentication-mode global on page 382](#) (set authentication to TACACS)
- primary-tacacs-ip (this command)
- [primary-tacacs-port on page 445](#) (designate port for primary TACACS server)
- [primary-tacacs-secret on page 447](#) (designate password for primary TACACS server)
- [authentication-type on page 384](#) tacacs+
- [secondary-tacacs-ip on page 460](#) (designate IP address of second TACACS+ server)
- [secondary-tacacs-port on page 462](#) designate port for second TACACS server)
- [secondary-tacacs-secret on page 464](#) (designate password for second TACACS server)

Examples

The following configures authentication for a TACACS+ server.

```
default(0)# configure terminal
default(0)(config)# authentication-mode global
default(0)(config-auth-mode)# primary-tac
primary-tacacs-ip      primary-tacacs-port  primary-tacacs-secret
default(0)(config-auth-mode)# primary-tacacs-ip 172.18.1.10
default(0)(config-auth-mode)# primary-tacacs-port 49
default(0)(config-auth-mode)# primary-tacacs-secret CSX2002
default(0)(config-auth-mode)# end

default(0)# show authentication-mode
```

Administrative User Management

```
AuthenticationType      : tacacs+
Primary RADIUS IP Address : 0.0.0.0
Primary RADIUS Port      : 1812
Primary RADIUS Secret Key : *****
Secondary RADIUS IP Address : 0.0.0.0
Secondary RADIUS Port      : 1812
Secondary RADIUS Secret Key : *****
Primary TACACS+ IP Address : 172.18.1.10
Primary TACACS+ Port      : 49
Primary TACACS+ Secret Key : *****
Secondary TACACS+ IP Address : 172.18.1.5
Secondary TACACS+ Port      : 49
Secondary TACACS+ Secret Key : *****
```

Related Commands

- [*authentication-mode global on page 382*](#)
- [*primary-tacacs-port on page 445*](#)
- [*primary-tacacs-secret on page 447*](#)
- [*authentication-type on page 384*](#)
- [*secondary-tacacs-ip on page 460*](#)
- [*secondary-tacacs-port on page 462*](#)
- [*secondary-tacacs-secret on page 464*](#)

primary-tacacs-port

Designates the port of the primary TACACS+ server.

Syntax

primary-tacacs-port <xx>

Command Mode

Configuration Mode > Authentication Mode

Default

NA

Usage

New commands to configure TACACS+ authentication mode for all administrators on a Cisco ACS server were introduced in FortiWLC (SD) 4.1:

- [authentication-mode global on page 382](#) (set authentication to TACACS)
- [primary-tacacs-ip on page 443](#) (designate IP address of primary TACACS+ server)
- [primary-tacacs-port on page 445](#) (designate port for primary TACACS server)
- [primary-tacacs-secret on page 447](#) (designate password for primary TACACS server)
- [authentication-type on page 384](#) tacacs+
- [secondary-tacacs-ip on page 460](#) (designate IP address of second TACACS+ server)
- [secondary-tacacs-port on page 462](#) (designate port for second TACACS server)
- [secondary-tacacs-secret on page 464](#) (designate password for second TACACS server)

Examples

The following configures authentication for a TACACS+ server.

```
default(0)# configure terminal
default(0)(config)# authentication-mode global
default(0)(config-auth-mode)# primary-tac
primary-tacacs-ip      primary-tacacs-port  primary-tacacs-secret
default(0)(config-auth-mode)# primary-tacacs-ip 172.18.1.10
default(0)(config-auth-mode)# primary-tacacs-port 49
default(0)(config-auth-mode)# primary-tacacs-secret CSX2002
default(0)(config-auth-mode)# end

default(0)# show authentication-mode
```

Administrative User Management

```
AuthenticationType      : tacacs+
Primary RADIUS IP Address : 0.0.0.0
Primary RADIUS Port      : 1812
Primary RADIUS Secret Key : *****
Secondary RADIUS IP Address : 0.0.0.0
Secondary RADIUS Port      : 1812
Secondary RADIUS Secret Key : *****
Primary TACACS+ IP Address : 172.18.1.10
Primary TACACS+ Port      : 49
Primary TACACS+ Secret Key : *****
Secondary TACACS+ IP Address : 172.18.1.5
Secondary TACACS+ Port      : 49
Secondary TACACS+ Secret Key : *****
```

Related Commands

- [*authentication-mode global on page 382*](#)
- [*primary-tacacs-ip on page 443*](#)
- [*primary-tacacs-secret on page 447*](#)
- [*authentication-type on page 384*](#)
- [*secondary-tacacs-ip on page 460*](#)
- [*secondary-tacacs-port on page 462*](#)
- [*secondary-tacacs-secret on page 464*](#)

primary-tacacs-secret

Designates the password of the primary TACACS+ server.

Syntax

primary-tacacs-ip <passwd>

Command Mode

Configuration Mode > Authentication Mode

Default

NA

Usage

New commands to configure TACACS+ authentication mode for all administrators on a Cisco ACS server were introduced in FortiWLC (SD) 4.1:

- [authentication-mode global on page 382](#) (set authentication to TACACS)
- [primary-tacacs-ip on page 443](#) (designate IP address of primary TACACS+ server)
- [primary-tacacs-port on page 445](#) (designate port for primary TACACS server)
- [primary-tacacs-secret on page 447](#) (designate password for primary TACACS server)
- [authentication-type on page 384](#) (for tacacs+)
- [secondary-tacacs-ip on page 460](#) (designate IP address of second TACACS+ server)
- [secondary-tacacs-port on page 462](#) (designate port for second TACACS server)
- [secondary-tacacs-secret on page 464](#) (designate password for second TACACS server)

Examples

The following configures authentication for a TACACS+ server.

```
default(0)# configure terminal
default(0)(config)# authentication-mode global
default(0)(config-auth-mode)# primary-tac
primary-tacacs-ip      primary-tacacs-port  primary-tacacs-secret
default(0)(config-auth-mode)# primary-tacacs-ip 172.18.1.10
default(0)(config-auth-mode)# primary-tacacs-port 49
default(0)(config-auth-mode)# primary-tacacs-secret CSX2002
default(0)(config-auth-mode)# end
```

```
default(0)# show authentication-mode
```

Administrative User Management

```
AuthenticationType      : tacacs+
Primary RADIUS IP Address : 0.0.0.0
Primary RADIUS Port      : 1812
Primary RADIUS Secret Key : *****
Secondary RADIUS IP Address : 0.0.0.0
Secondary RADIUS Port      : 1812
Secondary RADIUS Secret Key : *****
Primary TACACS+ IP Address : 172.18.1.10
Primary TACACS+ Port      : 49
Primary TACACS+ Secret Key : *****
Secondary TACACS+ IP Address : 172.18.1.5
Secondary TACACS+ Port      : 49
Secondary TACACS+ Secret Key : *****
```

Related Commands

- [*authentication-mode global on page 382*](#)
- [*primary-tacacs-port on page 445*](#)
- [*primary-tacacs-ip on page 443*](#)
- [*authentication-type on page 384*](#)
- [*secondary-tacacs-ip on page 460*](#)
- [*secondary-tacacs-port on page 462*](#)
- [*secondary-tacacs-secret on page 464*](#)

privilege-level

Configures local mode authentication privilege level for an admin.

Syntax `privilege-level <0,1,2,3,4,5,6,7,8>`

Command Mode Configuration Mode > Local Admin Mode

Default NA

Usage Use these commands to configure local administrators:

- [authentication-mode global on page 382](#)
- [authentication-type on page 384](#) (for local)
- [local-admin on page 433](#)
- password (only works in local-admin mode)
- privilege-level (only works in local-admin mode; only three numbers are used, 2, 5, and 8.)
- [show local-admins on page 480](#)

Numbers	Maps to...	Name and Priveleges
8	8	Operator is the lowest authentication level and also the default. Operatorscan see statistics and results but cannot make any configuration changes.
7	8	
6	8	
5	5	Admininstrators can also do general configuration changes, but cannot upgrade APs or controllers, nor can they upgrade FortiWLC (SD) versions using Telnet. The cannot configure an NMS server, NTP server, change the system password, date or time (all CLI). They cannot create local admins, a new feature in release 4.1, nor can they set the authentication mode for a controller (GUI and CLI). Administrators cannot add or remove licensing..
4	5	
3	5	

Numbers	Maps to...	Name and Priveleges
2	2	SuperUser administrators can perform all configurations on the controller. They are the only ones who can upgrade APs or controllers and they can upgrade FortiWLC (SD) versions using Telnet. They can configure an NMS server, NTP server, system password, date and time (all CLI). They can also create local admins, a new feature in release 4.1, and set the authentication mode for a controller (GUI and CLI). Superusers can add and remove licensing.
1	2	
0	2	

Examples

The following configures a local admin:

```
ramcntrl(0)# configure terminal
ramcntrl(0)(config)# authentication-mode global
ramcntrl(0)(config-auth-mode)# authentication-type local
ramcntrl(0)(config-auth-mode)# exit
ramcntrl(0)(config)# exit
ramcntrl(0)# sh authentication-mode
Administrative User Management
AuthenticationType : local
Primary RADIUS IP Address : 0.0.0.0
Primary RADIUS Port : 1812
Primary RADIUS Secret Key : *****
Secondary RADIUS IP Address : 0.0.0.0
Secondary RADIUS Port : 1812
Secondary RADIUS Secret Key : *****
Primary TACACS+ IP Address : 0.0.0.0
Primary TACACS+ Port : 49
Primary TACACS+ Secret Key : *****
Secondary TACACS+ IP Address : 0.0.0.0
Secondary TACACS+ Port : 49
Secondary TACACS+ Secret Key : *****
ramcntrl(0)#
ramcntrl(0)(config)# local-admin JCalhoun
ramcntrl(0)(config-local-admin)# privilege-level 2
ramcntrl(0)(config-local-admin)# password yosemite44
ramcntrl(0)(config-local-admin)# exit
```

```
ramcntrl(0)(config)# exit
```

Related Commands

- [local-admin](#) on page 433
- [password](#) on page 437

psk key

Sets a WPA-Personal or WPA2-Personal Passphrase (or “preshared key”).

Syntax

```
psk key <key>  
no psk key
```

key

A pre-shared key. The key can be from:

- 8 to 63 ASCII characters (the characters ! \ " ? must be escaped with the backslash (\) character; for example ! \ ?)
- 64 hex characters (hex keys must be prefixed with “0x” or the key will not work)

Command Mode

Security profile configuration mode.

Default

No key is set.

Usage

The Wi-Fi- Protected Access (WPA and WPA2) standard offers a more secure environment including improved and stronger authentication using 802.1X. If your site does not implement RADIUS servers, the WPA/WPA2 Passphrase is available as an improvement over the WEP64 and WEP128 shared key implementations.

The WPA-Personal and WPA2-Personal allow a longer shared secret key (256 bits) than that provided by WEP64 or WEP128. Assign one PSK per ESSID that uses this security profile. The key will be distributed to the ESSID APs. Clients joining the APs must have configured the same shared key prior to association.

Even though the Passphrase is more secure, managing the key is not automatic and presents some inconvenience because all client stations and APs in the WLAN need be updated each time the password changes. Passwords should be changed frequently to avoid detection.

WPA/WPA2 Passphrase can use keys containing either:

- 64 hexadecimal characters (that is, 0-9, a-f, A-F). Example: 0xa0a1a2a3a4a5a6a7a8a9aaabac or 0x12345678901234567890abcdef...
- 8 to 63 ASCII characters (the characters ! \ " ? must be escaped with the backslash (\) character; for example ! \ ?). Example: m6o0secret79\?key

Use the **no psk key** command to disable static WPA/WPA2 Passphrases.



If using a hexadecimal key, you must preface the key input with the 0x characters. The 0x characters notify the system that a hexadecimal key is being input.

Examples

The following command creates the WPA/WPA2 Passphrase:

```
controller(config-security)# psk key 012345678901234567890abcdef
```

Related Commands

[allowed-l2-modes](#) on **page 373**

radius-profile

Creates a profile for a Radius Server and enters Radius Server configuration mode.

Syntax

```
radius-profile <name>  
no radius-profile <name>
```

name	The name for the profiled RADIUS Server. The name can be from 1 to 16 characters long.
------	--

Command Mode

Global configuration mode

Default

No default.

Usage

This command creates a configuration profile for a Radius Server. The Radius Server is a key component of 802.1X WLAN security, as it provides access management by checking an access list to authenticate a user that attempts to join the WLAN. Many sites configure a primary and secondary Radius Server to ensure the continued availability of the authentication service, should the primary server become unavailable. The command **no radius-profile** deletes the profile.

From within the profile configuration, a Radius server IP address and passkey are required using the **ip-address** and **key** commands. Optional settings for description, port number, and record delimiter may also be specified using the **description**, **port**, and **mac-delimiter** commands. As well, in place of using the secret key, the MAC address of a client (as set in the RADIUS for MAC filtering configuration) can be used instead, as set with the **password-type** command.

After a RADIUS server profile is configured, use the **radius-server primary** or **radius-server secondary** command from within a security profile configuration to establish a relation to the newly configured profiles and determine the primary or secondary ranking of the server.

Radius profiles are also used for Radius accounting server configuration and MAC address ACLs (see the links in Related Commands section).

Examples

```
controller(config)# radius-profile main-auth  
controller(config-radius)# ?  
called-station-id-type (10) Configures the Called Station ID Type.
```

default	Set radius profile parameters to default value.
description	Specifies the radius node.
do	Executes an IOSCLI command.
end	Save changes, and return to privileged EXEC mode.
exit mode.	Save changes, and return to global configuration
ip-address	Configures the IP address.
key	Configures the secret key.
mac-delimiter	Configures the MAC Delimiter.
no	Disabling radius profile parameters.
password-type	Configures the RADIUS Password Type.
port	Configures port number.

Related Commands

- [*description on page 419*](#)
- [*ip-address on page 430*](#)
- [*key on page 431*](#)
- [*mac-delimiter on page 435*](#)
- [*port on page 442*](#)
- [*password on page 437*](#)
- [*accounting primary-radius on page 522*](#)
- [*accounting secondary-radius on page 524*](#)
- [*radius-server primary on page 456*](#)
- [*radius-server secondary on page 457*](#)

radius-server primary

Assigns and enables a primary RADIUS server specified in the profile.

Syntax

```
radius-server primary <profile>  
no radius-server primary  
no radius-server all
```

profile Specifies the name of the RADIUS server profile that was created with the **radius-profile** command.

Command Mode

Security Profile configuration

Usage

This command assigns and enables the primary RADIUS server specified in the profile that has been configured with the **radius-profile** command. Use this command as the last step in the RADIUS server configuration. The profile must exist before it can be assigned with this command.



Ensure the profile for RADIUS server configuration uses the appropriate port: 1812—RADIUS Authentication Server default port.

Use the **no radius-server all** command to disable the primary and secondary RADIUS servers or the **no radius-server primary** command to disable the primary RADIUS server.

Examples

The following command assigns the profile *main-auth* as the primary RADIUS server:

```
controller(config-security)# radius-server primary main-auth
```

Related Commands

- [radius-profile on page 454](#)
- [radius-server secondary on page 457](#)
- [show radius-profile on page 482](#)

radius-server secondary

Assigns and enables the secondary RADIUS server specified in the profile.

Syntax

```
radius-server secondary <profile>  
no radius-server secondary
```

profile Specifies the name of the RADIUS server profile that was created with the **radius-profile** command.

Command Mode

Security Profile configuration

Usage

This command assigns and enables the secondary RADIUS server specified in the profile that has been configured with the **radius-profile** command. Use the command as the last step in the RADIUS server setup. The profile must exist before it can be enabled with this command.

Use the command **no radius-server secondary** to disable the secondary RADIUS server.

Examples

The following command assigns the *backup-auth* profile as the secondary RADIUS server:

```
controller(config-security)# radius-server secondary backup-auth
```

Related Commands

- [radius-profile](#) on page 454
- [radius-server primary](#) on page 456
- [show radius-profile](#) on page 482

reauth

Enables reauthentication.

Syntax

```
reauth  
no reauth
```

Command Mode

Security Profile configuration

Default

Reauthentication is disabled.

Usage

This command causes the controller to honor and enforce the “Session-timeout” RADIUS attribute that may be present in a RADIUS Access-Accept packet.

Use this command if the Session-timeout attribute is used to require stations to reauthenticate to the network (802.1X) at a specified period. If “Session-timeout” is not used, there is no reason to enable Reauth in the Security Profile.

Examples

The following command enables reauthentication for the security profile.

```
controller(config-security)# reauth
```

Related Commands

| rekey period

Sets the interval for 802.1X key and WPA key regeneration.

Syntax

rekey period <*seconds*>
no rekey period

seconds Specifies the amount of time in seconds that an 802.1X key is valid. *seconds* can be a value between 0 and 65535.

Command Mode

Security Profile configuration

Default

The default rekey period is 0.

Usage

This command defines the length of time that an 802.1X key is valid. After the amount of time specified by *seconds* has elapsed, a new key is automatically generated. Frequently changing the key is recommended to prevent security breaches.

When 0 is specified, rekeying is disabled and the key is valid for the entire session, regardless of the session duration.

Use the **no rekey period** command to disable key regeneration.

Examples

The following command changes the key every 300 seconds (5 minutes):

```
controller(config-security)# rekey period 300
```

| Related Commands

[rekey period](#) on page 459

secondary-tacacs-ip

Designates the IP address of the second TACACS+ server.

Syntax

secondary-tacacs-ip <xx.xx.xx.xx>

Command Mode

Configuration Mode > Authentication Mode

Default

NA

Usage

New commands to configure TACACS+ authentication mode for all administrators on a Cisco ACS server were introduced in FortiWLC (SD) 4.1:

- [authentication-mode global on page 382](#) (set authentication to TACACS)
- [primary-tacacs-ip on page 443](#) (designate IP address of primary TACACS+ server)
- [primary-tacacs-port on page 445](#) (designate port for primary TACACS server)
- [primary-tacacs-secret on page 447](#) (designate password for primary TACACS server)
- [authentication-type on page 384](#) (for tacacs+)
- [secondary-tacacs-ip on page 460](#) (designate IP address of second TACACS+ server)
- [secondary-tacacs-port on page 462](#) (designate port for second TACACS server)
- [secondary-tacacs-secret on page 464](#) (designate password for second TACACS server)

Examples

The following configures authentication for a TACACS+ server.

```
default(0)# configure terminal
default(0)(config)# authentication-mode global
default(0)(config-auth-mode)# primary-tac
primary-tacacs-ip      primary-tacacs-port  primary-tacacs-secret
default(0)(config-auth-mode)# primary-tacacs-ip 172.18.1.10
default(0)(config-auth-mode)# primary-tacacs-port 49
default(0)(config-auth-mode)# primary-tacacs-secret CSX2002
default(0)(config-auth-mode)# end
```

```
default(0)# show authentication-mode
```


Administrative User Management

```
AuthenticationType      : tacacs+
Primary RADIUS IP Address : 0.0.0.0
Primary RADIUS Port      : 1812
Primary RADIUS Secret Key : *****
Secondary RADIUS IP Address : 0.0.0.0
Secondary RADIUS Port      : 1812
Secondary RADIUS Secret Key : *****
Primary TACACS+ IP Address : 172.18.1.10
Primary TACACS+ Port      : 49
Primary TACACS+ Secret Key : *****
Secondary TACACS+ IP Address : 172.18.1.5
Secondary TACACS+ Port      : 49
Secondary TACACS+ Secret Key : *****
```

Related Commands

- [*authentication-mode global on page 382*](#)
- [*primary-tacacs-port on page 445*](#)
- [*primary-tacacs-secret on page 447*](#)
- [*authentication-type on page 384*](#)
- [*secondary-tacacs-ip on page 460*](#)
- [*secondary-tacacs-port on page 462*](#)
- [*secondary-tacacs-secret on page 464*](#)

secondary-tacacs-port

Designates the port of the secondary TACACS+ server.

Syntax

secondary-tacacs-port <xx>

Command Mode

Configuration Mode > Authentication Mode

Default

NA

Usage

New commands to configure TACACS+ authentication mode for all administrators on a Cisco ACS server were introduced in FortiWLC (SD) 4.1:

- [authentication-mode global on page 382](#) (set authentication to TACACS)
- [primary-tacacs-ip on page 443](#) (designate IP address of primary TACACS+ server)
- [primary-tacacs-port on page 445](#) (designate port for primary TACACS server)
- [primary-tacacs-secret on page 447](#) (designate password for primary TACACS server)
- [authentication-type on page 384](#)
- [secondary-tacacs-ip on page 460](#) (designate IP address of second TACACS+ server)
- [secondary-tacacs-port on page 462](#) (designate port for second TACACS server)
- [secondary-tacacs-secret on page 464](#) (designate password for second TACACS server)

Examples

The following configures authentication for a TACACS+ server.

```
default(0)# configure terminal
default(0)(config)# authentication-mode global
default(0)(config-auth-mode)# primary-tac
primary-tacacs-ip      primary-tacacs-port  primary-tacacs-secret
default(0)(config-auth-mode)# primary-tacacs-ip 172.18.1.10
default(0)(config-auth-mode)# primary-tacacs-port 49
default(0)(config-auth-mode)# primary-tacacs-secret CSX2002
default(0)(config-auth-mode)# end
```

```
default(0)# show authentication-mode
```

Administrative User Management

```
AuthenticationType      : tacacs+
Primary RADIUS IP Address : 0.0.0.0
Primary RADIUS Port      : 1812
Primary RADIUS Secret Key : *****
Secondary RADIUS IP Address : 0.0.0.0
Secondary RADIUS Port      : 1812
Secondary RADIUS Secret Key : *****
Primary TACACS+ IP Address : 172.18.1.10
Primary TACACS+ Port      : 49
Primary TACACS+ Secret Key : *****
Secondary TACACS+ IP Address : 172.18.1.5
Secondary TACACS+ Port      : 49
Secondary TACACS+ Secret Key : *****
```

Related Commands

- [*authentication-mode global on page 382*](#)
- [*primary-tacacs-ip on page 443*](#)
- [*primary-tacacs-secret on page 447*](#)
- [*authentication-type on page 384*](#)
- [*secondary-tacacs-ip on page 460*](#)
- [*primary-tacacs-port on page 445*](#)
- [*secondary-tacacs-secret on page 464*](#)

secondary-tacacs-secret

Designates the password of the secondary TACACS+ server.

Syntax

primary-tacacs-ip <passwd>

Command Mode

Configuration Mode > Authentication Mode

Default

NA

Usage

New commands to configure TACACS+ authentication mode for all administrators on a Cisco ACS server were introduced in FortiWLC (SD) 4.1:

- [authentication-mode global on page 382](#) (set authentication to TACACS)
- [primary-tacacs-ip on page 443](#) (designate IP address of primary TACACS+ server)
- [primary-tacacs-port on page 445](#) (designate port for primary TACACS server)
- [primary-tacacs-secret on page 447](#) (designate password for primary TACACS server)
- [authentication-type on page 384](#) (for tacacs+)
- [secondary-tacacs-ip on page 460](#) (designate IP address of second TACACS+ server)
- [secondary-tacacs-port on page 462](#) (designate port for second TACACS server)
- [secondary-tacacs-secret on page 464](#) (designate password for second TACACS server)

Examples

The following configures authentication for a TACACS+ server.

```
default(0)# configure terminal
default(0)(config)# authentication-mode global
default(0)(config-auth-mode)# primary-tac
primary-tacacs-ip      primary-tacacs-port  primary-tacacs-secret
default(0)(config-auth-mode)# primary-tacacs-ip 172.18.1.10
default(0)(config-auth-mode)# primary-tacacs-port 49
default(0)(config-auth-mode)# primary-tacacs-secret CSX2002
default(0)(config-auth-mode)# end
```

```
default(0)# show authentication-mode
```

Administrative User Management

```
AuthenticationType      : tacacs+
Primary RADIUS IP Address : 0.0.0.0
Primary RADIUS Port      : 1812
Primary RADIUS Secret Key : *****
Secondary RADIUS IP Address : 0.0.0.0
Secondary RADIUS Port      : 1812
Secondary RADIUS Secret Key : *****
Primary TACACS+ IP Address : 172.18.1.10
Primary TACACS+ Port      : 49
Primary TACACS+ Secret Key : *****
Secondary TACACS+ IP Address : 172.18.1.5
Secondary TACACS+ Port      : 49
Secondary TACACS+ Secret Key : *****
```

Related Commands

- [*authentication-mode global on page 382*](#)
- [*primary-tacacs-port on page 445*](#)
- [*primary-tacacs-ip on page 443*](#)
- [*authentication-type on page 384*](#)
- [*secondary-tacacs-ip on page 460*](#)
- [*secondary-tacacs-port on page 462*](#)
- [*primary-tacacs-secret on page 447*](#)

security-logging

Turns security logging on and off.

Syntax

security-logging on
security-logging off

Command Mode

Security Profile configuration

Default

Security logging is **off**.

Usage

When security logging is on, logs are sent to syslog if the syslog-host is configured in the controller.

Examples

The following command turns security logging on on the controller named default:

```
default(config-security)# security-logging on
```

The following is an example of a syslog entry once security logging is enabled:

Station Connected details are logged as follows:

```
*****  
Feb 04 16:45:37 192.168.143.112 ALARM: 12022014871 | system | info | ALR |  
New Station Connected : MacAddress : 00:40:96:a3:5d:34, UserName : , AP-Id  
: 0, AP-Name : , BSSID : 00:12:F2:9b:02:01, ESSID : integ-mmode, Ip-Type :  
dynamic dhcp, Ip-Address : 0.0.0.0, L2mode : wpa2, L3-mode : clear, Vlan-  
Name : None, Vlan-Tag : 0
```

For example: Station Disconnected message would be as follows:

```
*****  
Feb 04 16:45:37 192.168.143.112 ALARM: 12022014871 | system | info | ALR |  
Station Disconnected : MacAddress : 00:40:96:a3:5d:34
```

Related Commands

- [firewall-filter-id](#) on page 426
- [syslog-host](#) on page 228

security-profile

Creates a security profile and enters security profile configuration mode.

Syntax

```
security-profile <name>  
no security-profile <name>
```

<i>name</i>	Unique text string up to 32 alphanumeric characters long. To use spaces and special characters, enclose them in double quotation marks (" ").
-------------	---

Command Mode

Global configuration

Default

The *default* security profile is provided.

Usage

The controller supports the ability to define multiple security profiles that can be assigned to different wireless LAN extended service sets (ESS) according to the level and type of security required. A security profile is a list of parameters that define how security is handled within an ESS. With security profiles, you can define the Layer 2 security method, including the cipher suite, primary and secondary RADIUS server, static WEP key entries and key index position, and other parameters. The various security profiles you create allow you to support multiple authentication and encryption methods within the same WLAN infrastructure.



Only one Layer 2 method can be defined in each security profile, although the same WEP key index settings can be used in several security profiles.

By default, FortiWLC (SD) contains a security profile named *default*, which uses OPEN authentication, meaning that there is no authentication, and that any wireless client can connect to the controller. The *default* profile is automatically associated with an ESSID when it is created.

Use the **no** form to delete a security profile. You can only delete a security profile if no ESSID specifies it. You cannot delete the *default* security profile.

Examples

The following commands create a security profile called *profile 1*, enter security profile configuration mode, and list the available commands:

```
controller(config)# security-profile "profile 1"
controller(config-security)#?
8021x-network-initiation (10) Enable 802.1x network initiation.
allowed-l2-modes          (10) Configure permitted L2 authentication modes.
captive-portal            (10) Enable captive portal.
captive-portal-auth-method (10) Configure captive portal authentication
method.
do                         (10) Executes an IOSCLI command.
encryption-modes          (10) Configure permitted cipher suites.
end                        (10) Save changes, and return to privileged EXEC
mode.
exit                      (10) Save changes, and return to global configuration
mod
e.
firewall-capability       (10) Configure Firewall Capability.
firewall-filter-id        (10) Configure Firewall Filter-ID.
group-rekey               (10) Configure the GroupRekey interval.
key-rotation              (10) Configure Key Rotation.
macfiltering              (10) Enable MAC Filtering.
no                         (10) Configure authentication parameters.
owner                     (10) Owner of the profile
passthrough-firewall-filter-id (10) Configure Passthrough Firewall Filter-
ID.
pmk-caching               (10) Enable PMK Caching.
psk                       (10) Configure the encryption WPA Pre-shared key
radius-server             (10) Configure RADIUS security.
reauth                    (10) Enable reauthentication.
rekey                     (10) Configure rekey period and related parameters.
security-logging          (10) Configure Security Profile Logging.
shared-authentication     (10) Enable shared authentication.
show                      (10) Displays various parameters.
static-wep                (10) Configure the static WEP key
tunnel-termination        (10) Configure Tunnel Termination.
```


Related Commands

- [ssid](#) on page 547
- [security-profile](#) on page 467
- [show security-profile](#) on page 484

shared-authentication

Enables shared authentication for additional security.

Syntax

```
shared-authentication enable  
no shared-authentication
```

Command Mode

Security profile configuration

Default

Shared authentication is off.

Usage

Use this command to enable shared authentication.

For networks that do not use WiFi Protected Access (WPA), you can use open authentication with Wireless Encryption Protocol (WEP) encryption. Use the **no shared-authentication** command to disable shared authentication with WEP. This helps provide additional security for your wireless network and helps protect your wireless network from intrusions by malicious users. If you use a shared key instead of open authentication with WEP encryption, the malicious user can easily decrypt the shared key to obtain access to all the computers in your wireless network.

Example

This example enables shared authentication:

```
Controller# configure terminal  
Controller(config)# security-profile wep64  
Controller(config-security)# allowed-l2-modes wep  
Controller(config-security)# encryption-modes wep64  
Controller(config-security)# static-wep key 12345  
Controller(config-security)# static-wep key-index 1  
Controller(config-security)# shared-authentication ?  
enable                Enable shared authentication.  
Controller(config-security)# shared-authentication enable  
Controller(config-security)# exit  
Controller(config)# end  
Controller#
```

Related Commands

security-profile on page 467

show aaa statistics

Displays detailed information about authentication statistics.

Syntax

show aaa statistics

Command Mode

EXEC

Usage

Use this command to view statistics about the 802.1X performance. The authentication statistics are reset when the controller is rebooted.

The aaa statistics are:

Statistic	Description
802.1x Authentication Request Count	Total number of 802.1x authentication requests.
802.1x Authentication Success Count	Number of successful authentication requests.
802.1x Authentication Failure Count	Number of failed authentication requests.
802.1x Authentication Station Count	Number of stations currently authenticated by 802.1x.

Examples

The following command shows 802.1X statistics:

```
controller# show aaa statistics
```

Authentication Statistics

802.1x Authentication Request Count : 519

802.1x Authentication Success Count : 54

802.1x Authentication Failure Count : 465

802.1x Authentication Station Count : 481

show access-list deny

Displays the list of MAC addresses in the deny ACL.

Syntax

show access-list deny

Command Mode

EXEC

Default

None

Usage

Use the **show access-list deny** command to see the deny list, which contains a list of MAC addresses that are denied access to the WLAN. In addition to creating a deny list, you must enable it before MAC addresses are denied. Only one list can be enabled at any given time; a permit and deny list cannot be enabled at the same time. You can create permit and deny lists and disable them, making MAC filtering inactive.

Examples

The following command displays the MAC addresses in the deny list:

```
controller# show access-list deny
```

```
MAC Address
```

```
00:0c:e6:bd:01:05
```

```
00:0c:e6:12:07:41
```

```
00:0c:e6:09:46:64
```

```
00:0c:30:be:f8:19
```

```
00:07:e9:15:69:40
```

```
00:06:25:a7:e9:11
```

```
00:04:23:87:89:71
```

```
ACL Deny Access Configuration (7 entries
```

```
controller#
```

Related Commands

- [access-list deny on page 363](#)
- [access-list deny import on page 365](#)

show access-list permit

Displays the list of MAC addresses in the permit ACL.

Syntax

show access-list permit

Command Mode

EXEC

Default

None

Usage

Use the **show access-list permit** command to see the permit list, which contains a list of MAC addresses that are permitted access to the WLAN. You must enable it before MAC addresses are permitted. Only one MAC filtering list can be enabled at any given time; a permit and deny list cannot be enabled at the same time. You can create permit and deny lists and disable them, making MAC filtering inactive.

Examples

The following command displays the list of MAC addresses in the permit list:

```
controller# show access-list permit
MAC Address
00:0c:e6:bd:01:05
00:0c:e6:12:07:41
00:0c:e6:09:46:64
00:0c:30:be:f8:19
00:07:e9:15:69:40
00:06:25:a7:e9:11
00:04:23:87:89:71
00:40:96:51:eb:2b
Acl Allow Access Configuration (8 entries)
controller#
```

Related Commands

- [access-list permit on page 367](#)
- [access-list permit import on page 369](#)

show air-shield

Displays the Air-Shield settings.

Syntax

show air-shield

Command Mode

Privileged EXEC

Usage

This command displays the settings for the Air-Shield features.

Examples

The following command displays the default Air-Shield settings:

```
controller# show air-shield
Air Shield

Air Firewall           : none
Allowed OUIs #1        : 00:00:00:00:00:00
Allowed OUIs #2        : 00:00:00:00:00:00
Allowed OUIs #3        : 00:00:00:00:00:00
Off-Hour Network Behaviour : none
Time Interval Start    : 00:00
Time Interval End      : 00:00
```

Related Commands

[access-list deny](#) on page 363

show arp

Displays the controller's ARP table with IP-MAC address mappings.

Syntax

show arp

Command Mode

Privileged EXEC

Default

NA

Usage

Examples

This example displays the controller's ARP table with IP-MAC address mappings:

```
corpwifi# show arp
```

Address Iface	HWtype	HWaddress	Flags	Mask
192.168.34.188	ether	00:22:10:B9:39:0C	CM	ats
192.168.34.65	ether	00:21:5C:08:EC:C7	CM	ats
192.168.34.44	ether	00:09:EF:07:56:AF	CM	ats
192.168.34.190	ether	00:22:10:B9:39:03	CM	ats
192.168.34.146		(incomplete)		controller
192.168.34.43	ether	00:21:6B:3B:61:A8	CM	ats
192.168.34.1	ether	00:19:BB:B0:27:00	C	controller
192.168.37.11	ether	00:1E:2A:36:04:B1	CM	ats
192.168.34.96		(incomplete)		ats
192.168.34.41	ether	00:24:B2:EF:C2:2A	CM	ats
192.168.34.74	ether	00:0C:E6:07:9F:3F	C	controller
192.168.34.147	ether	00:21:29:67:BB:96	CM	ats
192.168.34.37	ether	00:1C:BF:25:67:76	CM	ats
192.168.34.72	ether	00:1C:BF:25:A6:11	CM	ats
192.168.34.70	ether	00:0C:E6:04:3C:E8	C	controller
192.168.34.210	ether	00:03:25:40:86:EA	C	controller
192.168.34.101	ether	00:0C:E6:05:EA:FA	C	controller
192.168.34.179	ether	00:90:7A:08:A9:15	CM	ats

192.168.34.76	ether	00:16:6F:C7:2F:78	CM	ats
192.168.34.151	ether	00:16:EA:60:3C:C0	CM	ats
192.168.34.178	ether	00:01:3E:10:30:8B	CM	ats
192.168.34.150	ether	00:22:68:A0:EF:8D	CM	ats
192.168.34.117	ether	00:01:3E:10:1D:F7	CM	ats
192.168.37.31	ether	00:1B:2F:C5:A5:6B	CM	ats
192.168.34.24	ether	00:22:10:B9:39:07	CM	ats
192.168.34.174	ether	00:22:68:A0:F0:3B	CM	ats
192.168.34.25	ether	00:22:10:B9:39:21	CM	ats
192.168.34.51	ether	00:0C:E6:07:9F:11	C	controller
192.168.34.121	ether	00:0C:E6:04:DF:79	C	controller
192.168.34.120	ether	00:0C:E6:04:FC:E9	C	controller
192.168.34.28	ether	00:22:10:B9:39:08	CM	ats
192.168.34.171	ether	00:16:6F:0D:47:81	CM	ats
192.168.34.197	ether	00:25:4B:95:92:5A	CM	ats
192.168.34.58	ether	00:01:3E:10:1A:1D	CM	ats
192.168.34.30	ether	00:22:10:B9:38:FF	CM	ats

Related Commands

show authentication-mode

Displays the authentication-mode settings.

Syntax

show authentication-mode

Command Mode

Privileged EXEC

Usage

This command displays the settings that have been configured to determine where the Web User and Captive Portal Guest Users authentication is performed.

Examples

The following command shows that the RADIUS server named in the profile Primary is performing user authentication:

```
controller# show authentication-mode
auth_mode
```

```
AuthenticationType      : radius
Primary RADIUS Server   : Primary
Secondary RADIUS Server :
```

The following command shows that the controller is performing user authentication:

```
controller# show authentication-mode
auth_mode
```

```
AuthenticationType      : local
Primary RADIUS Server   :
Secondary RADIUS Server :
```

Related Commands

[authentication-mode](#) on page 380

show cef

Displays the Common Event Format Logging server configuration.

Syntax

show cef

Command Mode

Privileged EXEC

Default

NA

Usage

Use this command to display the configuration for the Common Event Format Logging server, as configured with the **cef** command.

Examples

The following shows the status of the logging server at 192.18.100.100:

```
default(config)# show cef
CEF Logging is disabled
Host      : 192.168.100.100
Port      : 514
```

Related Commands

[*cef*](#) on page 392

show local-admins

Lists the configured local administrators.

Syntax

`show local-admins`

Command Mode

Privileged EXEC

Default

NA

Usage

Use these commands, new in release 4.1, to configure local administrators:

- [authentication-mode global on page 382](#)
- [authentication-type on page 384](#) (for local)
- local-admin (this command)
- [password on page 437](#) (only works in local-admin mode)
- [privilege-level on page 449](#) (only works in local-admin mode)
- [show local-admins on page 480](#)

Examples

The following configures a local admin:

```
ramcntrl(0)# configure terminal
ramcntrl(0)(config)# authentication-mode global
ramcntrl(0)(config-auth-mode)# authentication-type local
ramcntrl(0)(config-auth-mode)# exit
ramcntrl(0)(config)# exit
ramcntrl(0)# sh authentication-mode
Administrative User Management
AuthenticationType : local
Primary RADIUS IP Address : 0.0.0.0
Primary RADIUS Port : 1812
Primary RADIUS Secret Key : *****
Secondary RADIUS IP Address : 0.0.0.0
Secondary RADIUS Port : 1812
```

```
Secondary RADIUS Secret Key : *****
Primary TACACS+ IP Address : 0.0.0.0
Primary TACACS+ Port : 49
Primary TACACS+ Secret Key : *****
Secondary TACACS+ IP Address : 0.0.0.0
Secondary TACACS+ Port : 49
Secondary TACACS+ Secret Key : *****
ramcntrl(0)#
ramcntrl(0)(config)# local-admin JCalhoun
ramcntrl(0)(config-local-admin)# privilege-level 2
ramcntrl(0)(config-local-admin)# password yosemite44
ramcntrl(0)(config-local-admin)# exit
ramcntrl(0)(config)# exit
```

Related Commands

- [password](#) on page 437
- [privilege-level](#) on page 449
- [local-admin](#) on page 433

show radius-profile

Displays the configured RADIUS profiles.

Syntax

```
show radius-profile
show radius-profile <name>
```

name Optional. Specifies the name of the profile to display.

Command Mode

Privileged EXEC

Default

A list of all RADIUS profiles is shown.

Usage

This command lists all RADIUS profiles that have been created with the **radius-profile** command, or with <name> added, lists the details of the *name* profile.

Examples

The following command displays configured RADIUS profiles:

```
controller# show radius-profile
```

Profile Name	RADIUS IP	Port	MAC Delimiter	Password Type
MyRad	192.168.100.1	1812	none	shared-secret

RADIUS Profile Table (1 entry)

The following command displays the MyRad RADIUS profile:

```
controller# show radius-profile MyRad
```

RADIUS Profile Table

RADIUS Profile Name	:MyRad
Description	:
RADIUS IP	:192.168.100.1
RADIUS Secret	:*****
RADIUS Port	:1812

MAC Address Delimiter :none
Password Type : shared-secret

Related Commands

[radius-profile](#) on page 454

show security-profile

Displays the configured security profiles.

Syntax

```
show security-profile <name>
```

name	Optional. Specifies the name of the profile to display.
------	---

Command Mode

Privileged EXEC

Default

A list of all security profiles is shown.

Usage

This command lists all security profiles that have been created with the **security-profile** command, or with the optional argument, lists the details of the profile specified by *name*.

Examples

The following command displays configured security profiles:

```
controller# show security-profile
# show security-profile
```

Profile Name	L2 Mode	Data Encrypt	Firewall Filter
Clear-CP	clear	none	ab10
wpa-psk	wpa-psk	tkip	
wpa2-peap	wpa2	ccmp	
wpa2-psk	wpa2-psk	ccmp	
wpa-peap	wpa	tkip	

Security Profile Table(5)


```

L2 Modes Allowed           : wpa-psk
Data Encrypt               : tkip
Primary RADIUS Profile Name :
Secondary RADIUS Profile Name :
WEP Key (Alphanumeric/Hexadecimal) : *****
Static WEP Key Index       : 1
Re-Key Period (seconds)    : 0
Enable Multicast Re-Key    : off
Enable Captive Portal      : disabled
802.1X Network Initiation  : on
Enable Shared Key Authentication : off
Pre-shared Key (Alphanumeric/Hexadecimal) : *****
Enable Reauthentication    : off
MAC Filtering              : on

```

controller# show security-profile wpapeap

```

Security Profile Name      : wpapsk
L2 Modes Allowed           : wpa-psk
Data Encrypt               : tkip
Primary RADIUS Profile Name :
Secondary RADIUS Profile Name :
WEP Key (Alphanumeric/Hexadecimal) : *****
Static WEP Key Index       : 1
Re-Key Period (seconds)    : 0
Captive Portal             : disabled
802.1X Network Initiation  : off
Shared Key Authentication   : off
Pre-shared Key (Alphanumeric/Hexadecimal) : *****
Group Keying Interval (seconds) : 0
PMK Caching                : disabled
Key Rotation               : disabled
Reauthentication           : off
MAC Filtering              : off
Firewall Capability        : none
Firewall Filter ID         :
Security Logging            : off
Security Profile Table

```

```
Security Profile Name           : wpapeap
L2 Modes Allowed                : wpa
Data Encrypt                    : tkip
Primary RADIUS Profile Name     : snow_ias
Secondary RADIUS Profile Name   :
WEP Key (Alphanumeric/Hexadecimal) : *****
Static WEP Key Index           : 0
Re-Key Period (seconds)        : 0
Enable Multicast Re-Key        : off
Enable Captive Portal          : disabled
802.1X Network Initiation      : on
Enable Shared Key Authentication : off
Pre-shared Key (Alphanumeric/Hexadecimal) : *****
Enable Reauthentication        : off
MAC Filtering                   : on
```

**Related
Commands**

[security-profile](#) on page 467

show ssl-server

Displays the configured SSL servers.

Syntax

show ssl-server

Command Mode

Privileged EXEC

Default

A list of all SSL servers is shown.

Usage

This command lists all SSL servers that are active.

Examples

The following command displays configured SSL servers:

```
controller# show ssl-server
SSL Server

Name                               : cp-ssl
Server Port                        : 10101
User Authentication Protocol       : None
Server Lifetime                    : 100
Server IP                          : 192.168.10.2
Certificate                        : controller.pem
RADIUS Profile Name                : cp-IAS
Secondary RADIUS Profile Name      :
CaptivePortalSessionTimeout        : 0
CaptivePortalActivityTimeout       : 0
Override RADIUS configurations    : off
```

Related Commands

- [ssl-server radius-profile on page 498](#)
- [ssl-server port on page 497](#)

show web

Displays web server Captive Portal configuration information.

Syntax

```
show web custom
show web custom-area
show web login-page
```

Command Mode

Privileged EXEC

Default

none

Usage

Use the command **show web custom** to display the IP range for Captive Portal custom mode.

Use the command **show web custom-area** to list the customized files for web-auth and Captive Portal.

Use the command **show web login-page** to display the type of page displayed for Captive Portal and WebAuth at client login. If the default login page is in use, the command returns the word **default**.

Examples

The following command shows the default Captive Portal/WebAuth login page is in use:

```
controller# show web login-page
```

```
default
```

This example directs a Captive Portal to customized pages and then shows the custom login page location:

```
MC3K-1(config)#
```

```
MC3K-1(config)# web custom ?
```

```
<attribute> Custom configurationn for attribute in captive portal.
```

```
MC3K-1(config)# web custom Auth_IP subnet 1.1.1.0 mask 255.255.255.0
```

```
MC3K-1(config)# web custom Guest_IP subnet 2.2.2.0 mask 255.255.255.0
```

```
MC3K-1(config)# exit
```

```
MC3K-1# show web custom ?
```

```
<attribute> Displays values of attribute in custom captive portal con
```

figuration.

```
MC3K-1# show web custom Auth_IP
```

```
1.1.1.0/24
```

```
MC3K-1# show web custom Guest_IP
```

```
2.2.2.0/24
```

Related Commands

[web login-page](#) on page 518

ssl-server accounting-radius-profile

Specifies the primary and secondary Radius server for Captive Portal accounting.

Syntax

```
ssl-server accounting-radius-profile primary <Radius server IP address>
ssl-server accounting-radius-profile secondary <Radius server IP address>
ssl-server no-primary-accounting-radius
ssl-server no-secondary accounting-radius
```

Command Mode Privileged EXEC

Default No primary or secondary Radius profile

Usage Use this command to specify the primary and secondary Radius server addresses used for Captive Portal accounting.

Examples This example assigns both a primary and secondary Radius accounting profile, and then removes both configurations.

```
Master(config)#
Master(config)# ssl-server accounting-radius-profile primary IAS
Master(config)# ssl-server accounting-radius-profile secondary IAS
Master(config)# end
Master#
Master# sh ssl-server
SSL Server
```

Name	: Captive Portal
Server Port	: 10101
User Authentication Protocol	: None
Server Lifetime	: 100
Server IP	: 192.168.106.153
Certificate	:
Primary RADIUS Profile Name	:
Secondary RADIUS Profile Name	:
Primary Accounting Radius Server Profile Name	: IAS

```
Secondary Accounting Radius Server Profile Name : IAS
Accounting Interim Interval (seconds)           : 600
CaptivePortalSessionTimeout                     : 0
CaptivePortalActivityTimeout                    : 0
CaptivePortal Authentication Type                : local-radius
Master# (config)
Master#(config)# ssl-server no-primary-accounting-radius
Master# (config)# ssl-server no-secondary-accounting-radius
```

Related Commands

[*captive-portal*](#) on page 388

ssl-server associate

This command is obsolete but it has not been blocked in this release. It specifies which configured certificate to associate with the SSL server. Instead of using this command, associate certificates to the Captive Portal service using the Web UI Management Server Certificate page.

Syntax

```
ssl-server associate pem <certificate>]
ssl-server associate pfx <certificate>]
```

certificate	Specifies the PEM or PFX certificate file name (a PEM uses the file extension pem and PFX uses the extension .pfx).
-------------	---

Command Mode

Global configuration

Default

NA

Usage

Specifies a PEM or PFX certificate file to be used with the SSL server. Configure these certificates from Web UI by importing the certificates and selecting them with Captive Portal.

Example

Related Commands

- [description on page 419](#)
- [ssl-server captive-portal on page 493](#)

Indicate that a third-party Captive Portal solution will be used in the Captive Portal configuration with the CLI command **ssl-server captive-portal-external-URL**. Then, provide the URL for the Captive Portal box with the command **change_mac_state**.

ssl-server captive-portal

Specifies the Captive Portal settings to use with the SSL server.

Syntax

```
ssl-server captive-portal activity-timeout <activity-timeout>
ssl-server captive-portal session-timeout <session-timeout>
ssl-server captive-portal authentication-type local
ssl-server captive-portal authentication-type radius override
```

activity-timeout	The number of minutes (between 0 and 60) of inactivity on a user session before the user is automatically logged off. By default, 0 is set, which is no timeout.
session-timeout	The number of minutes (between 0 and 1440 minutes) before a timeout is initiated for a station's active session. By default, 0 is set, which is no timeout.

Command Mode

Global configuration

Usage

If the **ssl-server captive-portal authentication-type local** command is used, the timeout values configured on the controller are used (session-timeout and activity-timeout parameters). For Captive Portal Authentication, only local guest users are valid.

Conversely, if the **ssl-server captive-portal authentication-type radius override** command is used, the timeout values configured in the Radius server are used (session-timeout and activity-timeout parameters). For Captive Portal Authentication, only Radius server users are valid.

If both local and Radius values are configured, local values are used. If no values are configured in the Radius server, controller values are used automatically. If no values are configured on the controller, the Radius server is not checked.

Example

This example sets session timeout to 600 minutes in the ssl-server page.

```
rao4038 # configure terminal
rao4038(config)# ssl-server captive-portal ?
activity-timeout    Configures activity-timeout for Captive Portal
authentication-type Configures authentication type for Radius configurations
```

session-timeout Configures session timeout period for Captive Portal
rao4038(config)# ssl-server captive-portal session-timeout 600
rao4038(config)#

Related Commands

- [ssl-server associate](#) on page 492
- [ssl-server port](#) on page 497
- [ssl-server radius-profile](#) on page 498

ssl-server captive-portal-external_URL

Works with [captive-portal-auth-method](#) on page 390 to indicate that a third-party Captive Portal authentication solution will be used.

Syntax

`ssl-server captive-portal-external_URL`

Command Mode

Configuration Mode, Security Mode

Default

Fortinet Captive Portal

Usage

Instead of using the Fortinet Captive Portal solution, you can use a third-party solution; you cannot use both. Companies such as Bradford, Avenda, and CloudPath all provide Captive Portal solutions that work with FortiWLC (SD) 4.1 and later. There are two places that you need to indicate a third-party captive portal solution, in the corresponding Security Profile and in the Captive Portal configuration. Indicate that a third-party Captive Portal solution will be used in the Security Profile with the CLI command **captive-portal-auth-method**. Indicate that a third-party Captive Portal solution will be used in the Captive Portal configuration with the CLI command **ssl-server captive-portal-external-URL**. Then, provide the URL for the Captive Portal box with the command **change_mac_state**.

Examples

This example configures third-party Captive Portal with the CLI by completing these two tasks:

Indicate that a third-party Captive Portal solution will be used in the Security Profile with the CLI command **captive-portal-auth-method**. For example:

```
controller1# configure terminal
controller1(config)# security-profile CPExternal
controller1(config-security)# captive-portal-auth-method
external internal
controller1(config-security)# captive-portal-auth-method ?
<captivePortAuthMethod> Configure captive portal authentication method.
external external
internal internal
controller1(config-security)# captive-portal-auth-method external
```

Indicate that a third-party Captive Portal solution will be used in the Captive Portal configuration with the CLI command **ssl-server captive-portal-external-URL**. Then, provide the URL for the Captive Portal box with the command **change_mac_state**. For example:

```
controller1# configure terminal
controller1(config)# ssl-server ca
captive-portal captive-portal-external-URL
controller1(config)# ssl-server captive-portal-external-URL
controller1(config)# exit
controller1# change_mac_state ?
<ip-address> Enter the Client IP Address.
controller1# change_mac_state 172.18.19.14 ?
off Web Auth mode off.
on Web Auth mode on.
controller1# change_mac_state 172.18.19.14 on ?
<CR>
<filter-id> Enter the Filter Id.
controller1# change_mac_state 172.18.19.14 on ftp_only
Configure a Radius Server for Captive Portal Authentication
© 2010 Fortinet, Inc. Captive Portals for Temporary Users 169
4.1 Beta
<CR>
controller1# change_mac_state 172.18.19.14 on ftp_only
controller1#
controller1# change_mac_state 172.18.19.14 ?
off Web Auth mode off.
on Web Auth mode on.
controller1# change_mac_state 172.18.19.14 off ?
<CR>
<filter-id> Enter the Filter Id.
controller1# change_mac_state 172.18.19.14 off
controller1
```

Related Commands

- [captive-portal-auth-method](#) on page 390
- [change_mac_state](#) on page 416

ssl-server port

Specifies the SSL server's TCP port number.

Syntax

ssl-server port <port-number>

port-number TCP port number in the range of 1024 through 65,535.

Command Mode

Global configuration

Default

The default port number for the SSL server is 10101.

Usage

Specifies the SSL server's TCP port number.

Examples

The following command specifies the SSL server's port number as 12345:

```
controller(config)# ssl-server port 12345  
controller(config)#
```

Related Commands

- [ssl-server associate](#) on page 492
- [ssl-server captive-portal](#) on page 493
- [ssl-server radius-profile](#) on page 498

ssl-server radius-profile

Sets the RADIUS profile name where RADIUS server parameters are configured.

Syntax

```
ssl-server radius-profile primary <profile-name>  
ssl-server radius-profile secondary <profile-name>  
ssl-server no-1st-radius  
ssl-server no-2nd-radius
```

profile-name

Names the file containing the RADIUS server configuration information. Text string of up to 32 alphanumeric characters. Do not use spaces.

Command Mode

Global configuration

Default

NA

Usage

This command specifies the RADIUS profile name where the RADIUS server parameters for a primary or secondary RADIUS server are specified for use by the SSL server.

The **ssl-server no-1st-radius** command disables a previously configured primary RADIUS profile for use by the SSL server.

The **ssl-server no-2nd-radius** command disables a previously configured secondary RADIUS profile for use by the SSL server.

Examples

The following command configures the SSL Server to use the primary RADIUS server settings profile *main*:

```
controller(config)# ssl-server radius-profile primary main  
controller(config)#
```

Related Commands

- [radius-profile](#) on page 454
- [ssl-server associate](#) on page 492
- [ssl-server captive-portal](#) on page 493
- [ssl-server port](#) on page 497

ssl-server cna-bypass

Enable or disable Apples' CNA support.

Syntax `ssl-server cna-bypass [on | off]`

Command Mode Global configuration

Default Off (Disabled)

Usage When enabled, the auto-login pop-up is not displayed in a captive portal authentication (in tunnelled mode) using an Apple device.

Examples The following command enables Apple CNA bypass.

```
mc3200(15)# configure terminal
master(15)(config)# ssl-server cna-bypass on
master(15)(config)# exit
master(15)# sh ssl-server
Captive Portal
Name : Captive Portal
Configuring Fortinet Captive Portal 239
Server Port : 10101
User Authentication Protocol : None
Server Lifetime : 100
Server IP : 172.18.34.177
Certificate :
Authentication Type : radius
Primary Profile :
Secondary Profile :
Primary Profile :
Secondary Profile :
Accounting Interim Interval (seconds) : 600
CaptivePortalSessionTimeout : 0
```

CaptivePortalActivityTimeout : 0
Protocol : https
Portal URL :
CaptivePortal External URL :
CaptivePortal External IP : 172.18.34.177
L3 User Session Timeout(mins) : 1
Apple Captive Network Assistant (CNA) Bypass : on

Related Commands

- [*radius-profile*](#) **on page 454**
- [*ssl-server associate*](#) **on page 492**
- [*ssl-server captive-portal*](#) **on page 493**
- [*ssl-server port*](#) **on page 497**

static-wep key

Configures a static WEP key.

Syntax

```
static-wep key <key>  
no static-wep key
```

key

- For WEP64, the key is a 5-character ASCII or 10-character hex key.
- For WEP128, the key must be 13 ASCII characters or 26 hex digits.

Command Mode

Security profile configuration

Default

None

Usage

802.11 WEP (wired equivalent privacy) uses MAC-level encryption of data between a mobile unit and an AP. Once the frame enters the wired side of the network, such as between access points, WEP no longer applies.

WEP64, also known as WEP40, is more widespread and uses keys containing either:

- 10 hexadecimal characters (that is, 0-9,a-f, A-F). Example: 0x0123456789
- 5 ASCII characters (all keyboard characters). Example: 01234 or mykey

WEP128 is more secure though not as widespread and uses keys containing either:

- 26 hexadecimal characters (that is, 0-9,a-f, A-F). Example: 0xa0a1a2a3a4a5a6a7a8a9aaabac or 0x12345678901234567890abcdef
- 13 ASCII characters (all keyboard characters). Example: my-secret-key

Use the **no static-wep key** command to disable static WEP keys.



If using a hexadecimal key, you must preface the key input with the 0x characters. The 0x characters notify the system that a hexadecimal key is being input.

Examples

The following command specifies a WEP key of *wpass*:

```
controller(config-security)# static-wep key wpass  
controller(config-security)#
```

Related Commands

- [encryption-modes wep128](#) on page 423
- [encryption-modes wep64](#) on page 424
- [static-wep key-index](#) on page 503

static-wep key-index

Configures the index position of a static WEP key.

Syntax

`static-wep key-index <position>`

position Static WEP key index position. *position* may be from 1 to 4.

Command Mode

Security profile configuration

Default

Usage

This command specifies the use of one of the four possible static WEP keys that can be configured by the user station key management program. The key index feature provides interoperability if the user program can configure four key settings.

Examples

The following command specifies that the third WEP key be used:

```
controller(config-security)# static-wep key-index 3
controller(config-security)#
```

Related Commands

- [static-wep key on page 501](#)
- [encryption-modes wep128 on page 423](#)
- [encryption-modes wep64 on page 424](#)
- [security-profile on page 467](#)

tunnel-termination

Tunnel-Termination is provided by IOSCLI and Controller GUI, to perform configuration on per-security profile basis.

Syntax `tunnel-termination <PEAP/TTLS>`

Command Mode Security profile configuration

Default Termination is off

Usage Tunnel termination allows the controller to terminate the PEAP/TTLS outer session on the controller. The inner MSCHAPv2 802.1x is handled by the backend radius server. This is useful when the radius server does not support PEAP or TTLS.

Examples The following command disables the tunnel termination:

```
controller(config-security)# no tunnel-termination (peap/ttls)
controller(config-security)#
```



The following L2 Modes are supported only for the PEAP or TTLS authentication protocol:

- 802.1x
 - WPA
 - WPA2
 - Mixed
-

vpn client

Allows you to configure the properties of the VPN connection between the controller and the Network Manager server.

Syntax

vpn client

Command Mode

Global configuration

Default

NA

Usage

This command is used to view and configure the properties of the VPN configuration to the Network Manager appliance. Several subcommands are executed from within this configuration setting.

Examples

```
default(15)# configure terminal
default(15)(config)# vpn client
default(15)(config-vpn-client)# ?
  do (10) Executes an IOSCLI command.
  end (10) Save changes, and return to privileged EXEC mode.
  exit (10) Save changes, and return to global configuration mode.
  no (10) Disables various parameters.
  vpn-client-state (10) Enables VPN Client.
  vpn-server-ip (10) Configures the VPN Server IP address.
  vpn-server-port (10) Configures the VPN Server port number.
default(15)(config-vpn-client)#
```

Related Commands

- [\(config-vpn-client\) vpn-client-state on page 506](#)
- [\(config-vpn-client\) vpn-server-ip on page 507](#)
- [\(config-vpn-client\) vpn-server-port on page 508](#)

(config-vpn-client) vpn-client-state

Allows you to enable or disable VPN communication between the controller and the Network Manager server.

Syntax

```
(config-vpn-client) vpn-client-state  
(config-vpn-client) no vpn-client-state
```

Command Mode

VPN client configuration

Default

Disabled

Usage

This command is used to activate or deactivate the VPN connection to the Network Manager server.

Examples

The example below enables and then disables the VPN server.

```
default(15)(config-vpn)# vpn-client-state  
default(15)(config-vpn)#  
default(15)(config-vpn)# no vpn-client-state  
default(15)(config-vpn)#
```

Related Commands

- [vpn client on page 505](#)
- [\(config-vpn-client\) vpn-server-ip on page 507](#)
- [\(config-vpn-client\) vpn-server-port on page 508](#)

(config-vpn-client) vpn-server-ip

Allows you to configure the IP address for the VPN-enabled Network Manager server.

Syntax

(config-vpn-client) vpn-server-ip <IP>

IP Specify an IP (in the format 255.255.255.255).

Command Mode

VPN client configuration

Default

NA

Usage

This command is used to specify the IP address of the VPN server.

Examples

```
default(15)(config-vpn-client)# vpn-server-ip 10.9.8.7
default(15)(config-vpn-client)# end
```

Related Commands

- [vpn client](#) on page 505
- [\(config-vpn-client\) vpn-client-state](#) on page 506
- [\(config-vpn-client\) vpn-server-port](#) on page 508

(config-vpn-client) vpn-server-port

Allows you to specify the port to be used for the VPN service.

Syntax

(config-vpn-client) vpn-server-port <port>

Port Specify a port (any integer from 0 to 65535).

Command Mode

VPN client configuration

Default

1194

Usage

This command is used to specify the port to be utilized by the VPN client configuration.

Examples

```
default(15)(config-vpn-client)# vpn-server-port 1194
default(15)(config-vpn-client)# end
```

Related Commands

- [vpn client](#) on page 505
- [\(config-vpn-client\) vpn-client-state](#) on page 506
- [\(config-vpn-client\) vpn-server-ip](#) on page 507

vpn server

Allows you to configure the properties of the VPN server.

Syntax

vpn server

Command Mode

Global configuration

Default

NA

Usage

This command is used to view and configure the properties of the VPN configuration hosted on the controller. Several subcommands are executed from within this configuration setting.

Examples

```
default(15)# configure terminal
default(15)(config)# vpn server
default(15)(config-vpn)# ?
do (10) Executes an IOSCLI command.
encryption (10) Enables Encryption.
end (10) Save changes, and return to privileged EXEC mode.
exit (10) Save changes, and return to global configuration mode.
ip-pool (10) Configures the IP Pool address.
no (10) Disables various parameters.
port (10) Configures the VPN Server port number.
subnet-mask (10) Configures the subnet mask.
vpn-server-ip (10) Configures the VPN Server IP address.
vpn-server-state (10) Enables VPN Server.
default(15)(config-vpn)#
```

Related Commands

- [\(config-vpn\) encryption on page 510](#)
- [\(config-vpn\) ip-pool on page 511](#)
- [\(config-vpn\) port on page 512](#)
- [\(config-vpn\) subnet-mask on page 513](#)
- [\(config-vpn\) vpn-server-ip on page 514](#)
- [\(config-vpn\) vpn-server-state on page 515](#)

(config-vpn) encryption

Allows you to enable or disable VPN encryption.

Syntax

(config-vpn) encryption

Command Mode

VPN configuration

Default

Enabled

Usage

This command is used to activate or deactivate encryption on the controller's VPN configuration.

Examples

The example below enables and then disables encryption.

```
default(15)(config-vpn)# encryption
default(15)(config-vpn)#
default(15)(config-vpn)# no encryption
default(15)(config-vpn)#
```

Related Commands

- [vpn server on page 509](#)
- [\(config-vpn\) ip-pool on page 511](#)
- [\(config-vpn\) port on page 512](#)
- [\(config-vpn\) subnet-mask on page 513](#)
- [\(config-vpn\) vpn-server-ip on page 514](#)
- [\(config-vpn\) vpn-server-state on page 515](#)

(config-vpn) ip-pool

Allows you to specify the IP pool to be used for the VPN service.

Syntax

(config-vpn) ip-pool <IP>

IP Specify an IP range (in the format 255.255.255.255).

Command Mode

VPN configuration

Default

192.168.0.0

Usage

This command is used to specify the range of IPs that can be utilized by the VPN configuration.

Examples

```
default(15)(config-vpn)# ip-pool 192.168.100.0
default(15)(config-vpn)# end
```

Related Commands

- [vpn server on page 509](#)
- [\(config-vpn\) encryption on page 510](#)
- [\(config-vpn\) port on page 512](#)
- [\(config-vpn\) subnet-mask on page 513](#)
- [\(config-vpn\) vpn-server-ip on page 514](#)
- [\(config-vpn\) vpn-server-state on page 515](#)

(config-vpn) port

Allows you to specify the port to be used for the VPN service.

Syntax

(config-vpn) port <port>

Port Specify a port (any integer from 0 to 65535).

Command Mode

VPN configuration

Default

1194

Usage

This command is used to specify the port to be utilized by the VPN configuration.

Examples

```
default(15)(config-vpn)# port 1194
default(15)(config-vpn)# end
```

Related Commands

- [vpn server on page 509](#)
- [\(config-vpn\) encryption on page 510](#)
- [\(config-vpn\) ip-pool on page 511](#)
- [\(config-vpn\) subnet-mask on page 513](#)
- [\(config-vpn\) vpn-server-ip on page 514](#)
- [\(config-vpn\) vpn-server-state on page 515](#)

(config-vpn) subnet-mask

Allows you to specify the subnet mask to be used for the VPN service.

Syntax

(config-vpn) subnet-mask <netmask>

Netmask Specify an IP (in the format 255.255.255.255).

Command Mode

VPN configuration

Default

255.255.0.0

Usage

This command is used to specify the subnet mask to be utilized by the VPN configuration.

Examples

```
default(15)(config-vpn)# subnet-mask 255.255.255.0
default(15)(config-vpn)# end
```

Related Commands

- [vpn server on page 509](#)
- [\(config-vpn\) encryption on page 510](#)
- [\(config-vpn\) ip-pool on page 511](#)
- [\(config-vpn\) port on page 512](#)
- [\(config-vpn\) vpn-server-ip on page 514](#)
- [\(config-vpn\) vpn-server-state on page 515](#)

(config-vpn) vpn-server-ip

Allows you to configure the IP address to be used for the VPN service.

Syntax

(config-vpn) vpn-server-ip <IP>

IP Specify an IP (in the format 255.255.255.255).

Command Mode

VPN configuration

Default

NA

Usage

This command is used to specify the IP address of the VPN server.

Examples

```
default(15)(config-vpn)# vpn-server-ip 10.9.8.7
default(15)(config-vpn)# end
```

Related Commands

- [vpn server on page 509](#)
- [\(config-vpn\) encryption on page 510](#)
- [\(config-vpn\) ip-pool on page 511](#)
- [\(config-vpn\) port on page 512](#)
- [\(config-vpn\) subnet-mask on page 513](#)
- [\(config-vpn\) vpn-server-state on page 515](#)

(config-vpn) vpn-server-state

Allows you to enable or disable the VPN service.

Syntax (config-vpn) vpn-server-state
 (config-vpn) no vpn-server-state

Command Mode VPN configuration

Default Disabled

Usage This command is used to activate or deactivate the VPN service on the controller.

Examples The example below enables and then disables the VPN server.

```
default(15)(config-vpn)# vpn-server-state
default(15)(config-vpn)#
default(15)(config-vpn)# no vpn-server-state
default(15)(config-vpn)#
```

- Related Commands**
- [vpn server on page 509](#)
 - [\(config-vpn\) encryption on page 510](#)
 - [\(config-vpn\) ip-pool on page 511](#)
 - [\(config-vpn\) port on page 512](#)
 - [\(config-vpn\) subnet-mask on page 513](#)
 - [\(config-vpn\) vpn-server-ip on page 514](#)

web custom

Configures captive portal custom mode.

Syntax

```
web custom CaptivePortal1 landing-file-name<name.html> success-file-name
<name.html>
web custom CaptivePortal2 landing-file-name<name.html> success-file-name
<name.html>
```

Command Mode

Configuration Mode

Default

None

Usage

Use **web custom** to configure up to four captive portal custom file names.

Use the command [web login-page on page 518](#) to select either default or custom login pages for web-authentication and Captive Portal. Indicate the names of custom pages with the command [web custom on page 516](#). Use the command **show web custom** to list files that are used for Captive Portal/WebAuth implementation. If the default login page is in use, the command lists the **empty.html** and **empty.gif** files.

Examples

The following command shows the default Captive Portal/WebAuth login page is in use:

```
controller# show web login-page
default
```

This example directs Captive Portal to customized files and then shows the custom login page location:

```
MC3K-1# configure terminal
MC3K-1(config)# web custom ?
CaptivePortal1      Custom configuration for captive portal 1
CaptivePortal2      Custom configuration for captive portal 2
MC3K-1(config)# web custom captiveportal2 ?
landing-file-name  subnet
MC3K-1(config)# web custom CaptivePortal2 landing-file-name landing.html
success-file-name  success.html
```



```
MC3K-1 (config) web custom CaptivePortal2 subnet 1.1.1.0 mask
255.255.255.0
MC3K-1(config)# exit
MC3K-1# show web ?
custom                Displays IP range for captive portal custom mode.
custom-area           Lists the files in the custom area for web-auth and
capti
ve portal.
login-page            Displays the type of login page used for web-auth
and cap
tive portal.
MC3K-1# show web custom
Insufficient parameters for command
MC3K-1# show web custom-area
Html Files
total 16
-rw-rw-rw-    1 root    root        2607 Jul 13 16:26 page20K.html
-rw-rw-rw-    1 root    root        4412 Jul 13 16:26 page2LOGIN.html
-rwx-----    1 root    root        2607 Jul 13 16:04 auth_web_ok.html
-rw-rw-rw-    1 root    root        4412 Jul 13 16:04 loginformWeb-
Auth.html
-rwx-----    1 root    root            0 Jun 30 00:31 empty.html
Image Files
total 9
-rwx-----    1 root    root            0 Jun 30 00:31 empty.gif
-rw-rw-rw-    1 root    root       8574 Oct 29  2008 Sample.jpg
MC3K-1# show web login-page
custom
```

**Related
Commands**

[show web](#) on page 488

web login-page

Selects either the default or custom Captive Portal/WebAuth login page.

Syntax

```
web login-page default
web login-page custom
```

Command Mode

Global configuration mode.

Default

Fortinet default login page.

Usage

Use the command **web login-page** to select either default or custom login pages for web-authentication and Captive Portal. Indicate the names of custom pages with the command [web custom on page 516](#). Use the command **show web custom** to list files that are used for Captive Portal/WebAuth implementation. If the default login page is in use, the command lists the **empty.html** and **empty.gif** files.



You must use the Web UI to download the generic files, modify them, and then upload customized .html and .gif files for the custom option to work. From the **Detailed > Maintenance > Captive Portal** area, click the Customization link and the Get Files button to obtain the files. Once you have modified the generic files, use the Import Files link to upload the files. Then to activate the pages, use the command **web login-page custom** or go to the Customization link Step 2--Change the Mode and select the Customized radio button.

Use the **web login-page default** change to the default login page.

Related Commands

- [web custom on page 516](#)
- [show web on page 488](#)

10 ESSID Commands

The commands contained in this chapter are used to create and manage ESSs. Included are commands that enable/disable features such as Radius accounting, **Remote APs**, and VLANs. Also included are many commands that allow fine-tuning of the default broadcast settings for implementations with unique requirements. Profiles created by E(z)RF Network Manager can not be modified/deleted by a controller. You can unregister a controller from Network Manager using the CLI command **nms-server unregister**. After unregistering a configuration, the controller becomes the owner of a copy of the profile and can then edit or delete profiles created with Network Manager.

- [*accounting interim-interval*](#) on page 521
- [*accounting primary-radius*](#) on page 522
- [*accounting secondary-radius*](#) on page 524
- [*ap-discovery join-ess*](#) on page 526
- [*ap-discovery join-virtual-ap*](#) on page 527
- [*apsd*](#) on page 531
- [*band-steering-mode*](#) on page 533
- [*band-steering-timeout*](#) on page 534
- [*base-tx-rates*](#) on page 536
- [*beacon dtim-period*](#) on page 538
- [*beacon period*](#) on page 539
- [*bssid*](#) on page 540
- [*calls-per-bss*](#) on page 541
- [*countermeasure*](#) on page 542
- [*dataplane*](#) on page 543
- [*edited-bssid*](#) on page 545
- [*ess-ap*](#) on page 546
- [*essid*](#) on page 547
- [*gre name*](#) on page 548
- [*l2bridge airf*](#) on page 549

- [*l2bridge appletalk*](#) on page 550
- [*l2bridge ipv6*](#) on page 551
- [*multicast-enable*](#) on page 552
- [*multicast-mac-transparency*](#) on page 553
- [*overflowfrom-essprofile*](#) on page 554
- [*publish-essid*](#) on page 556
- [*security-profile*](#) on page 557
- [*show edited-bssid*](#) on page 559
- [*show ess-ap*](#) on page 558
- [*show essid*](#) on page 560
- [*ssid*](#) on page 563
- [*supported-tx-rates*](#) on page 564
- [*tunnel-type*](#) on page 566
- [*virtual-port*](#) on page 567
- [*vlan name*](#) on page 568
- [*wireless-to-wireless-isolation*](#) on page 569

accounting interim-interval

Specifies the amount of time that elapses before the controller sends an Interim-Update record to the RADIUS accounting server.

Syntax

accounting interim-interval <value>

<i>value</i>	Number of seconds that elapse before Interim-Update records are sent. The interval must be from 600 through 36,000 seconds (10 minutes through 10 hours).
--------------	---

Command Mode

ESSID configuration

Default

The default accounting interim interval value is 3,600 seconds.

Usage

If RADIUS accounting is enabled, the controller sends an Accounting-Start record to the RADIUS accounting server after receiving an Access-Accept response from the RADIUS server. When the client session times out or the client is disassociated, the controller sends an Accounting-Stop record to the RADIUS server. If the Access-Accept response contained the Acct-Interim-Interval attribute, the controller sends Interim-Update records at the interval configured with the **accounting interim-interval** command for the duration of the client session.

Examples

The following command sets the accounting interim interval to 1,800 seconds (30 minutes):

```
controller(config-ssid)# accounting interim-interval 1800
controller(config-ssid)#
```

Related Commands

- [accounting primary-radius](#) on page 522
- [accounting secondary-radius](#) on page 524

accounting primary-radius

Specifies the primary RADIUS Accounting server.

Syntax

```
accounting primary-radius <profile>  
no accounting-radius all
```

profile Name of the RADIUS Accounting server profile, specified with the **radius-profile** command.

Command Mode

ESSID configuration

Default

Communication between the controller and the primary RADIUS accounting server is disabled by default.

Usage

Use the **accounting primary-radius** command to set up and enable communications between the controller and the primary RADIUS Accounting server.

When RADIUS Accounting is enabled, the controller sends accounting records to the RADIUS Accounting server for clients who authenticate using 802.1X. (To see a list of the accounting attributes that are tracked, see the “Configuring RADIUS Accounting,” and “Configuring Multiple ESSIDs,” in the **FortiWLC-SD Configuration Guide**.)



Do not use the RADIUS Authentication Server for this configuration. The Authentication Server configuration will not work, as the RADIUS Accounting Server uses port 1813 instead of port 1812.

RADIUS Accounting server configuration information, such as IP address, port (1813 is the standard port for accounting), and secret key, is specified using the **radius-profile** command.

Use the **no accounting-radius all** command to disable the accounting primary radius server.

Examples

The following command sets the server information in the profile *main-acct* for the primary RADIUS accounting server:

```
controller(config-ssid)# accounting primary-radius main-acct  
controller(config-ssid)#
```

Related Commands

- [*accounting interim-interval*](#) **on page 521**
- [*radius-profile*](#) **on page 454**
- [*accounting secondary-radius*](#) **on page 524**

accounting secondary-radius

Specifies the secondary RADIUS accounting server.

Syntax

```
accounting secondary-radius <profile>  
no accounting-radius secondary  
no accounting-radius all
```

profile

Name of the RADIUS server profile, specified with the **radius-profile** command.

Command Mode

ESSID configuration

Default

Communication between the controller and the secondary RADIUS accounting server is disabled by default.

Usage

You can specify a secondary RADIUS accounting server that the controller sends accounting records to if the primary RADIUS accounting server is offline. Use the **accounting secondary-radius** command to enable communications with the secondary RADIUS accounting server.

Use **no accounting-radius secondary** or **no accounting-radius all** to disable communication with the secondary RADIUS accounting server.

When RADIUS accounting is enabled, the controller sends accounting records to the RADIUS accounting server for clients who authenticate using 802.1X. (To see a list of the accounting attributes that are tracked, see the “Configuring RADIUS Accounting,” and “Configuring Multiple ESSIDs,” in the **FortiWLC-SD Configuration Guide**.)

RADIUS accounting server configuration information, such as IP address, port (1813 is the standard port for accounting), and secret key, is specified using the **radius-profile** command.

Examples

The following command sets the server information in the profile *backup-acct* for the secondary RADIUS accounting server:

```
controller# configure terminal  
controller(config) essid eng  
controller(config-ssid)# accounting secondary-radius backup-acct
```



```
controller(config-ssid)#
```

Related Commands

- [*accounting interim-interval*](#) **on page 521**
- [*radius-profile*](#) **on page 454**
- [*accounting primary-radius*](#) **on page 522**

ap-discovery join-ess

Configures whether new access points automatically join an ESSID and are configured with its parameters.

Syntax

```
ap-discovery join-ess
no ap-discovery join-ess
```

Command Mode

ESSID configuration

Default

Enabled

Usage

By default, the **join-ess-on-discovery** command is enabled, which means that access points automatically join an ESSID and a BSS is automatically created. When a new access point is plugged into the WLAN, it goes through all the ESSIDs and joins all of them that have **ap-discovery join-ess** enabled. When creating an ESSID, access points join the new ESSID.

After you are satisfied with your WLAN configuration, you can disable **ap-discovery join-ess** so that new access points do not change your configuration. If you are adding a new ESS that you want to advertise on only a small subset of access points, it is easier to create the ESS with **ap-discovery join-ess** disabled and add the ESS-AP mappings manually.

Use the **no** form to prevent access points from automatically joining an ESSID. If the **no** form is used, a BSSID must be assigned manually.

Examples

The following command disables **ap-discovery join-ess**, which prevents access points from automatically joining an ESSID:

```
controller# configure terminal
controller(config) essid eng
controller(config-essid)# no ap-discovery join-ess
controller(config-essid)#
```

Related Commands

- [ssid](#) on page 563
- [show essid](#) on page 560

ap-discovery join-virtual-ap

Enables access points discovered on the same channel to share the same BSSID, forming a Virtual Cell.

Syntax `ap-discovery join-virtual-ap`
 `no ap-discovery join-virtual-ap`

Command Mode ESSID configuration

Default Enabled

Usage By default, the **ap-discovery join-virtual-ap** command is enabled when creating an ESSID. This allows the formation of a Virtual Cell, which is a group of access points on the same channel sharing the same BSSID. If the **ap-discovery join-virtual-ap** command is disabled, access points on the same channel cannot share the same BSSID, which prevents the formation of a Virtual Cell. When the **ap-discovery join-virtual-ap** command is disabled, each access point has its own unique BSSID.



This status of this command is only evaluated when new ESS-AP mappings are created. ESS-AP mappings are either created manually with the **ess-ap** command, or automatically when a new ESS is created, or a new access point is discovered.

Use the **no** form to disable access points on the same channel from sharing the same BSSID. Some examples of when you disable **ap-discovery join-virtual-ap**:

- You do not want to create a Virtual Cell. (In other words, each access point has its own BSSID.)
- You require access point recognition by BSSID.

Examples The following command disables **ap-discovery join-virtual-ap**, which prevents access points on the same channel to share the same BSSID:

```
controller# configure terminal
controller(config) essid eng
controller(config-essid)# no ap-discovery join-virtual-ap
controller(config-essid)#
```

Related Commands

- [ess-ap](#) on page 546
- [show essid](#) on page 560

ap-vlan priority

Used with bridged VLANs to give a tagged VLAN top priority.

Syntax

```
ap-vlan-priority
no ap-vlan-priority
```

Command Mode

ESSID configuration

Default

NA

Usage

Bridged mode ESS profiles are supported by AP300, AP400, and AP1000 models. Indicate that an ESS profile is bridged with the command **dataplane**. A VLAN tag can then be configured for a profile with the command **ap-vlan-tag** and then multiple profiles can be associated to that VLAN tag. The command **ap_vlan_priority** raises the priority of a tagged VLAN. This setting indicates whether an AP needs to map incoming VLAN 802.1p data packets into WMM ACs or not. By default in bridged ESS, this is disabled, and an AP always honors DSCP in IPV4 packets to map an incoming packet to one of WMM ACs. When you turn this on, an AP honors VLAN 802.1p priority over DSCP priority when the packet is mapped into one of WMM ACs.

Example

This example creates the ESSID abcjk, sets its mode to bridged, assigns a tag, and then gives top priority to abcjk.

```
test(config-essid)#
test# configure terminal
test(config)# essid abcjk
test(config-essid)# dataplane bridged
test(config-essid)# ap-vlan-tag 11
test(config-essid)# ap-vlan-priority
test(config-essid)# end
```

Related Commands

- [ap-vlan-tag](#) on page 530
- [dataplane](#) on page 543

ap-vlan-tag

Assigns a tag to a bridged VLAN.

Syntax

```
ap-vlan-tag <number>  
no ap-vlan-tag <number>
```

Command Mode

ESSID configuration

Default

NA

Usage

Bridged mode ESS profiles are supported by AP300, AP400, and AP1000 models. Indicate that an ESS profile is bridged with the command **dataplane**. A VLAN tag can then be configured for a profile with the command **ap-vlan-tag** and then multiple profiles can be associated to that VLAN tag. The command **ap-vlan priority** raises the priority of a tagged VLAN.

Example

This example creates the ESSID abcjk, sets its mode to bridged, assigns a tag, and then gives top priority to abcjk.

```
test(config-ssid)#  
test# configure terminal  
test(config)# ssid abcjk  
test(config-ssid)# dataplane bridged  
test(config-ssid)# ap-vlan-tag 11  
test(config-ssid)# ap-vlan-priority  
test(config-ssid)# end
```

Related Commands

- [ap-vlan priority on page 529](#)
- [dataplane on page 543](#)

apsd

When APSD is on for an ESS, the AP buffers frames while devices are using power save and transmits the frames when the device comes back online.

Syntax

```
apsd-support  
no apsd-support
```

Command Mode

ESSID configuration

Default

APSD settings are configured per ESS and APSD support is **on** by default.

Usage

WMM is an enhancement to legacy power save that allows devices to save power while improving performance and minimizing transmission latency. To accomplish this, U-APSD capable stations download frames buffered at AP300s during unscheduled Service Periods (SP); the result is that there is no wait for beacons as there is in the legacy method. For U-APSD capable stations, AP300 negotiates U-APSD and uses it to transmit data when a station is in power-save mode. When a device comes out of power-save mode, the uplink data frame triggers AP300 to send frames buffered in trigger/delivery enabled queues. Pending legacy mode frames are not transmitted. Check for the APSD configuration by issuing the command **show station**.

Example

This example turns off WMM-APSD support for the ESSID named APSD:

```
default# configure terminal  
default(config)# essid apsd  
default(config-essid)# no apsd-support  
default(config-essid)# end  
default(config)# end  
default# show station 802.11 mac-address 00:00:4c:5a:e9:94  
Station Database 802.11 Table  
MAC Address           : 00:00:4c:5a:e9:94  
AP ID                  : 56  
AP Name                : AP-56  
Interface Index       : 0  
ESSID                  : pk1
```

BSSID	: 00:0c:e6:f6:bf:d3
Virtual Port	: 06:0b:0d:5a:e9:94
RF Band	: 802.11g
Capabilities	: wmm,apsd
Last Associated time	: 11/11/2009 16:38:33
Last Handoff time	: 11/11/2009 16:33:08
Neighboring AP Count	: 0
Transmitted Throughput	: 530
Received Throughput	: 105
Current RSSI	: -43
Loss Percentage	: 76
Channel Utilization	: 0

band-steering-mode

Directs ESS traffic to band A or band N for dual-band-capable clients.

Syntax

```
band-steering-mode a-steering  
band-steering-mode n-steering  
band-steering-mode disable
```

Command Mode

Configuration ESSID

Default

Band steering is disabled by default.

Usage

Band steering balances multi-band capable clients by assignments bands to clients based on their capabilities. Without band steering, an ABG client could formerly associate on either the A or the B/G channels, leading to overcrowding on one band or the other. With band steering, you can leave all voice-capable clients on the B/G channels (where bandwidth is not a concern) and move data-only clients to the A band to achieve higher data rates. To use band steering for ABGN traffic, you could use A-steering to direct dual mode clients with A capability to the 5 GHz band and use N-steering to direct all dual mode clients with AN capability to the 5 GHz band. Band steering is also useful for directing multicast traffic. For this command to work as clients are added, also set the field New APs Join ESS to **on** in the ESS (see the command [essid on page 547](#)).

Example

This example sets band steering to the A channel on the existing ESS named BandSteeringTest and then sets the band steering timeout to 7 seconds (see [band-steering-timeout on page 534](#)):

```
DemoController# configure terminal  
DemoController(config)# essid bandSteeringTest  
DemoController(config-essid)# band-steering-mode a-steering  
DemoController(config-essid)# band-steering-timeout 7  
DemoController(config-essid)# end
```

Related Commands

- [band-steering-timeout on page 534](#)
- [essid on page 547](#)

band-steering-timeout

Sets the number of seconds that assignment for a steered client is blocked on the forbidden band while it is unassociated.

Syntax `band-steering-timeout <seconds>`

Command Mode Configuration ESSID

Default The default is 5 seconds.

Usage Sets the number of seconds that assignment for a steered client is blocked on the forbidden band while it is unassociated. For this command to work, also set the field Band Steering to A-band or N-band.

Example This example sets remote-ap-enable, sets band steering to the A channel, and then sets band steering timeout to 10 seconds for the ESS named Bandsteeress:

```
default# configure terminal
default(config)# essid Bandsteeress
default(config-ssid)# dataplane
default(config-ssid)# remote-ap-enable
default(config-ssid)# band-steering-mode a-steering
default(config-ssid)# band-steering-timeout 10
default(config-ssid)# end
```

This example sets band steering to the A channel on the existing ESS (see [band-steering-mode on page 533](#)) named BandSteeringTest and then sets the band steering timeout to 7 seconds:

```
DemoController# configure terminal
DemoController(config)# essid bandSteeringTest
DemoController(config-ssid)# band-steering-mode a-steering
DemoController(config-ssid)# band-steering-timeout 7
DemoController(config-ssid)# end
```

Related Commands

- [band-steering-mode](#) on page 533
- [essid](#) on page 547

base-tx-rates

Sets base transmit rates (Mbps).

Syntax

```
base-tx-rates 802.11a all
base-tx-rates 802.11a <rate>
base-tx-rates 802.11b all
base-tx-rates 802.11b <rate>
base-tx-rates 802.11bg all
base-tx-rates 802.11bg <rate>
base-tx-rates 802.11g all
base-tx-rates 802.11g <rate>
base-tx-rates 802.11bg all
base-tx-rates 802.11bg <rate>
base-tx-rates 802.11bgn all
base-tx-rates 802.11bgn <rate>
base-tx-rates 802.11an all
base-tx-rates 802.11an <rate>
```

Default values are:

- B Supported Transmit Rates (Mbps): 1,2,5.5,11
- B Base Transmit Rates (Mbps): 11
- A Supported Transmit Rates (Mbps): 6,9,12,18,24,36,48,54
- A Base Transmit Rates (Mbps): 6,12,24
- G Supported Transmit Rates (Mbps): 6,9,12,18,24,36,48,54
- G Base Transmit Rates (Mbps): 6,9,12,18,24,36,48,54
- BG Supported Transmit Rates (Mbps): 1,2,5.5,11,6,9,12,18,24,36,48,54
- BG Base Transmit Rates (Mbps): 11
- BGN Supported Transmit Rates (Mbps): 1,2,5.5,11,6,9,12,18,24,36,48,54
- BGN Base Transmit Rates (Mbps): 11
- BGN Supported HT Transmit Rates (MCS): 0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
- BGN Base HT Transmit Rates (MCS): none
- AN Supported Transmit Rates (Mbps): 6,9,12,18,24,36,48,54
- AN Base Transmit Rates (Mbps): 6,12,24
- AN Supported HT Transmit Rates (MCS): 0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
- AN Base HT Transmit Rates (MCS): none

Command Mode

ESS configuration

Usage

Setting the base rate specifies the mandatory rates that all connecting clients must support when connecting to the access point. Except when the **all** argument is used, each base rate change (either when adding or deleting) must be implemented with a separate command; that is, you cannot configure several rates using one command (for example, **base-tx-rate 802.11bg 1 2 11** is invalid).

Use the **no** form of the command to disable a specified base rate. Changing the base rate in an ESS profile will cause all clients on all ESSIDs to reassociate.

The supported data rates are the rates supported by the access points. The base data rates are a subset of the supported rates. The access point first tries to transmit at the highest data rate set to Basic. If there are problems encountered in the transmission, the access points steps down to the highest rate that allows data transmission.

Examples

The following command sets the 802.11bg base transmit rate to 11:

```
controller# configure terminal
controller(config) essid eng
default(config-essid)# base-tx-rate 802.11bg 11
```

The following command sets the 802.11a base transmit rate to support all rates (1, 2, 5.5, 11, 6, 9, 12, 18, 24, 36, 48, and 54 Mbps) :

```
controller# configure terminal
controller(config) essid eng
default(config-essid)# base-tx-rate 802.11a all
```

Related Commands

[*supported-tx-rates*](#) on page 564

beacon dtim-period

Sets the intervals at which beacons are sent.

Syntax

beacon dtim-period *<period>*

period

Number of beacon intervals that elapse before broadcast frames stored in buffers are sent. The beacon interval must be 20-1000 milliseconds. For AP300 and AP208 the beacon interval is a multiple of 20, from 20 to 1000ms. For OAP 180, the beacon interval is a multiple of 100, from 100 to 500ms.

Command Mode

ESS configuration

Default

The default beacon DTIM period is 1.

Usage

Setting the DTIM period to a higher value decreases the frequency of broadcasts sent by the access point. If power-save mode is enabled on clients that are connected to access points, clients “wake up” less if fewer broadcasts are sent, which conserves battery life for the clients.

Because broadcasts are generally wasteful of air resources, FortiWLC (SD) replaces broadcasts with more efficient, limited unicasts. Therefore, only the behavior of clients currently in power-save mode is affected by the DTIM period value.

Examples

The following command changes the beacon DTIM period to 20:

```
controller# configure terminal
controller(config) essid eng
default(config-essid)# beacon dtim-period 20
default(config-essid)#
```

Related Commands

- [essid on page 547](#)
- [show essid on page 560](#)

beacon period

Sets the rate at which beacons are transmitted.

Syntax

beacon period <period>

period

Number of TUs (1 TU=1.024 ms) between beacons. Value must be between 20 and 1000 milliseconds (and a multiple of 20 for AP300 models).

Command Mode

ESSID configuration

Default

The default beacon period is 100 TUs.

Usage

Setting the beacon period to a higher value decreases the frequency of unicasts and broadcasts sent by the access point. If power-save mode is enabled on clients that are connected to access points, clients “wake up” less if fewer unicasts and broadcasts are sent, which conserves battery life for the clients. The beacon period setting affects unicasts and broadcasts.

Examples

The following command changes the beacon period to 200 TUs:

```
controller# configure terminal
controller(config) essid eng
controller(config-ssid)# beacon period 200
controller(config-ssid)#
```

Related Commands

[show essid](#) on page 560

bssid

Sets the BSSID for an ESS on a specific access point.

Syntax

bssid <*bssid*>

bssid Unique MAC address in hexadecimal format (*nn:nn:nn:nn:nn:nn*).

Command Mode

ESS-AP configuration

Default

None

Usage

By default, all access points in the FortiWLC (SD) are assigned random MAC addresses as BSSIDs. Each BSSID must be a unique value across the WLAN. Additionally, all access points on the same channel are given the same BSSID by default. Access points with the same BSSID automatically work together to form a Virtual Cell for that BSSID. Each Virtual Cell appears as one access point to the clients, and provides the benefits of seamless hand-off, load balancing, and optimal client assignment without “ping-ponging.”

Use the **bssid** command to override the default BSSID assigned to an access point. When you change the BSSID, the BSSID for all access points on that channel that do not have a BSSID that has been overridden are changed.

Examples

The following command sets the BSSID to 00:0c:e6:02:7c:84:

```
controller# configure terminal
controller(config) essid eng
controller(config-essid-essap)# bssid 00:0c:e6:02:7c:84
controller(config-essid-essap)#
```

Related Commands

- [show ess-ap on page 558](#)
- [show edited-bssid on page 559](#)

calls-per-bss

Sets the maximum number of voice calls for this BSSID.

Syntax

calls-per-bss <*calls*>

calls Sets the maximum number of voice calls for this BSSID. The allowable range of calls is from 0 to 999. Setting *calls* to 0 uses the value for the global setting of **qosvars calls-per-bssid**.

Command Mode

ESS-AP configuration

Default

Calls is set to 0.

Usage

This command is similar to the global QoS command, **qosvars calls-per-bssid**, but allows you to configure the maximum number of calls for this BSSID only. When both commands are used, the setting from this command takes precedence.

This command, with an argument other than the default (0), sets a threshold for the maximum number of calls for this BSS. This command implements the Call Admission Control (CAC) feature, which ensures a consistent level of voice quality by setting a threshold for the number of calls allowed. As the set threshold is reached, CAC denies new SIP connections until enough bandwidth is available to effectively handle the resulting media stream

When the call limit for this BSS is exceeded, all new calls receive a 486_BusyHere response until the number of calls is under the specified threshold.

Examples

The following command sets the maximum number of calls for this BSSID to 14:

```
controller# configure terminal
controller(config) essid eng
controller (config-essid)ess-ap 3 1
controller(config-essid-essap)# calls-per-bss 14
```

Related Commands

[qosvars calls-per-bssid](#) on page 729

countermeasure

Enables and disables MIC countermeasures.

Syntax

```
countermeasure  
no countermeasure
```

Command Mode

ESSID configuration

Default

Countermeasures are enabled by default.

Usage

The **countermeasure** command lets you selectively enable or disable MIC countermeasures for each ESSID. MIC countermeasures are on by default. They should only be turned off temporarily with the **no countermeasure** command while a network administrator identifies and then resolves the source of a MIC error.

Countermeasures are helpful if an AP encounters two consecutive MIC errors from the same client within a 60 second period. The AP will disassociate all clients from the ESSID where the errors originated and does not allow any clients to connect for 60 seconds. This prevents an MIC attack.

When countermeasures are disabled, any packets that have MIC errors are dropped, but clients are not disassociated, even if the offending station continues to send packets to the AP that has MIC errors.

Example

This example disables countermeasure for the ESSID jaypsk2, then configures it.

```
Master# configure terminal  
Master(config)# essid jaypsk2  
Master(config-ssid)# no countermeasure  
Master(config-ssid)# countermeasure  
Master(config-ssid)# exit
```

dataplane

Use this command to support bridging with VLAN on AP300. This command replaced remote-ap-enable in release 4.0.

Syntax

dataplane bridged

dataplane tunneled

bridged	Specifies the data packets are not passed to the controller; only control plane packets are passed to the controller (Remote AP mode).
tunneled	Specifies the default behavior for APs where data and control packets are passed to the controller (default).

Command Mode

ESSID configuration

Default

The default is tunneled traffic.

Usage

This command determines the type of traffic passed between the controller and an AP. By default, tunneled mode is active where a controller and an AP are connected with a data tunnel so that data from a mobile station is tunneled to the controller from an AP and vice versa.

When bridged mode is used, an AP can be installed and managed at a location separated from the controller by a WAN or ISP, for example a satellite office. The controller monitors remote APs with a keep-alive signal. Remote APs exchange control information, including authentication and accounting information, with the controller but cannot exchange data. Remote APs exchange data with other APs within their subnet.

Because remote APs cannot exchange data-plane traffic (including DHCP) with the controller, these FortiWLC (SD) features are not available for Remote AP configuration: Virtual Cell, VLAN, Captive Portal, L3 Mobility, and QoS.

To secure the bridged connection over the public airwaves, use the AP Configuration mode command dataplane-encryption on command.

Bridged mode ESS profiles are supported by AP300s. Indicate that an ESS profile is bridged with the command dataplane. A VLAN tag can then be configured for a profile with the command ap-vlan-tag and then multiple profiles can be associated to that VLAN tag. The command ap_vlan_priority raises the priority of a tagged VLAN.

Examples

This example creates the ESSID abcjk, sets its mode to bridged, assigns a tag, and then gives top priority to abcjk.

```
test(config-ssid)#  
test# configure terminal  
test(config)# ssid abcjk  
test(config-ssid)# dataplane bridged  
test(config-ssid)# ap-vlan-tag 11  
test(config-ssid)# ap-vlan-priority  
test(config-ssid)# end
```

Related Commands

- [ap-vlan priority](#) on page 529
- [ap-vlan-tag](#) on page 530

edited-bssid

Syntax edited-bssid <ap-id> <ifindex> <essid> <bssid>

Command Mode Global configuration

Default Disabled

Usage

Examples

```
default# configure terminal
default(config)# edited-bssid 11 1 Asvin_test 00:0c:e6:01:06:11
default(config)# edited-bssid 12 1 Asvin_test 00:0c:e6:01:06:12
default(config)# exit
default# show edited-bssid
```

AP ID	IfIndex	ESS	Profile	BSSID
11	1		Asvin_test	00:0c:e6:01:06:11
12	1		Asvin_test	00:0c:e6:01:06:12

Edited BssID Entry(2 entries)

```
default#
```

Related Commands [show edited-bssid](#) on page 559

ess-ap

Assigns an access point to an ESS and enters ESS-AP configuration mode.

Syntax

ess-ap <ap-id> <interface_index>

ap-id ID number of the AP to associate with the ESS.

interface_index The wireless interface index of the AP.

Command Mode

ESSID configuration

Default

None

Usage

Use this command to assign an access point to an ESS and enter ESS-AP configuration mode, where you can assign the BSSID of the channel for the access point and calls per BSS.

Examples

The following configures AP-3, index 1:

```
controller# configure terminal
controller(config) essid eng
controller (config-essid)ess-ap 3 1
controller(config-essid-essap)#
```

Related Commands

- [show ess-ap on page 558](#)
- [bssid on page 540](#)
- [calls-per-bss on page 541](#)

ssid

Creates or deletes an extended service set ID (ESSID).

Syntax

```
ssid <ssid>  
no ssid <ssid>
```

ssid String of up to 32 alphanumeric characters long.

Command Mode

Global configuration

Default

None

Usage

The ESSID is the name of a WLAN that clients see and connect to. By default, all access points that join the ESS and have the same channel form a Virtual Cell.

The maximum number of ESSIDs you can create for FortiWLC (SD) is 64.

By default, any new ESSIDs are configured to use the security profile named *default*. To use another security profile, create it, and then assign it to the ESSID using the **security-profile** command in the ESSID configuration mode.

This value must be the same as the name assigned to the SSID name.

Use the **no** form to delete an ESSID.

Examples

The following command creates an ESSID named *sj_engineering*:

```
controller# configure terminal  
controller(config)# ssid sj_engineering  
controller(config-ssid)#
```

Related Commands

- [show ssid on page 560](#)
- [ssid on page 563](#)

gre name

Assigns a GRE profile to an ESSID.

Syntax

`gre name <name>`

Command Mode

ESSID configuration

Default

None

Usage

When creating an ESSID, you can assign a GRE to the ESSID. This allows you to use the a GRE tunnel with the ESSID. By default, ESSIDs do not have GRE tunnels assigned to them. You must create a GRE profile using the `gre` command in global configuration mode before assigning the GRE name to an ESSID. As well, use the `tunnel-type` command to assign the tunnel-type of GRE to the ESSID.

Examples

The following command assigns the corp GRE to an ESSID:

```
controller# configure terminal
controller(config) essid eng
controller(config-ssid)# gre name corp
controller(config-ssid)# tunnel-type GRE
```

Related Commands

- [gre](#) on page 342
- [tunnel-type](#) on page 566

12bridge airf

These commands enable and disable airf bridging.

Syntax

```
12bridge airf  
no 12bridge airf
```

Command Mode

ESSID configuration

Default

Airf bridging is disabled and Air Fortress is disabled by default.

Usage

FortressTech Layer 2 bridging and encryption with Fortress Technology AirFortress gateway allow an administrator to configure FortressTech encryption on one or more ESSIDs. From the essid configuration submode, use the commands **12bridge airf** and **no 12bridge airf** to enable and disable airf bridging, respectively.

Examples

The following command turns off airf bridging on the controller named eng:

```
eng(config)# configure terminal  
eng(config)# ssid sj_engineering  
eng(config-ssid)# no 12bridge airf
```

Related Commands

[ssid](#) on page 547

12bridge appletalk

Enable and disable AppleTalk bridging.

Syntax

```
12bridge appletalk  
no 12bridge appletalk
```

Command Mode

ESSID configuration

Default

Appletalk is disabled by default.

Usage

Use the commands **12bridge appletalk** and **no 12bridge appletalk** to enable and disable AppleTalk bridging, respectively. If more than one ESSID profile is active on the controller, AppleTalk clients are not able to find an enabled AppleTalk printer. This does not occur when only one ESSID is active.

Examples

The following command turns off AppleTalk on the controller eng:

```
eng(config)# essid guest  
eng(config-ssid)# no 12bridge appletalk
```

Related Commands

[essid](#) on page 547

l2bridge ipv6

Enables protocol bridging of IPv6 traffic.

Syntax

```
l2bridge ipv6  
no l2bridge ipv6
```

Command Mode

ESSID configuration

Default

IPv6 bridging is disabled by default.

Usage

With ipv6 bridging, neither the AP nor the controller actually participate (are not actual end-points) in an IPv6/AppleTalk/AirF network; the protocols are simply bridged or passed through the Fortinet infrastructure and are transparent to those networks. Fortinet devices don't actually get an IPv6/AppleTalk address nor process packets but just passes them from transmitter to receiver.

Example

The following command turns off IPv6 on the controller eng:

```
eng # configure terminal  
eng(config)# essid guest  
eng(config-ssid)# no l2bridge ipv6
```

To turn on IPv6 on the controller eng:

```
eng # configure terminal  
eng(config)# essid guest  
eng(config-ssid)# l2bridge ipv6
```

multicast-enable

Enables multicast for an ESSID.

Syntax

multicast-enable
no multicast-enable

Command Mode

ESSID configuration

Default

Multicast is disabled by default.

Usage

Use the **multicast-enable** command if you need to broadcast the same stream, such as video, to multiple stations. Enabling multicast causes all multicast packets on the air side to appear on the wired side and all multicast packets on the wired side to appear on the air side.

Use the **no** form to disable multicast.



Multicast is an advanced feature. Enabling multicast in the WLAN can cause subtle changes in your network. Be sure to consult with your network administrator prior to enabling this feature.

Examples

The following command enables multicast.

```
controller# configure terminal
controller(config) ssid eng
controller(config-ssid)# multicast-enable
```

Related Commands

[show ssid](#) on page 560

multicast-mac-transparency

Enables MAC transparency for tunneled multicast.

Syntax

```
multicast-mac-transparency  
no multicast-mac-transparency
```

Command Mode

ESSID configuration

Default

Multicast is disabled by default; multicast transparency is disabled by default.

Usage

Use the multicast-mac-transparency command to support visibility of wired stations' source MAC addresses. A wired station's source MAC address is propagated to the wireless clients in the source mac address field of the multicast packets.

Examples

The following command enables multicast and then enables multicast-mac-transparency.

```
controller# configure terminal  
controller(config) essid eng  
controller(config-ssid)# multicast-enable  
controller(config-ssid)# multicast-mac-transparency
```

Related Commands


[multicast-enable](#) on page 552

overflowfrom-essprofile

Example:

```
default(0)# show essid
ESS Profile Name          SSID          Security
Profile                  Broadcast Tunnel Interface Type
vcelloverflow            vcelloverflow          default
on                        none
                        ESS Profile(1 entry)
default(0)# configure terminal
default(0)(config)# essid vcelloverflowoss
default(0)(config-essid)# overflowfrom-essprofile <ess profile name>
default(0)(config-essid)# end
default(0)# show essid
ESS Profile Name          SSID          Security
Profile                  Broadcast Tunnel Interface Type
vcelloverflow            vcelloverflow          default
on                        none
vcelloverflowoss         vcelloverflow          default
on                        none
                        ESS Profile(2)
default(0)# show essid vcelloverflowoss
ESS Profile

ESS Profile Name          : vcelloverflowoss
SSID                      : vcelloverflow
Security Profile Name     : default
Primary RADIUS Accounting Server :
Secondary RADIUS Accounting Server :
Accounting Interim Interval (seconds) : 3600
Beacon Interval (msec)    : 100
SSID Broadcast            : on
Bridging                  : none
New AP's Join ESS         : on
Tunnel Interface Type     : none
VLAN Name                 :
GRE Tunnel Profile Name   :
```

Allow Multicast Flag	: off
Virtual Cell	: off (overflow ESS must not be VC)
Virtual Port	: off
ESS Profile Name for Overflow from	: vcellooverflow
	
APSD Support	: off
DTIM Period (number of beacons)	: 1
Dataplane Mode	: tunneled
AP VLAN Tag	: 0
AP VLAN Priority	: off
Countermeasure	: on
Multicast MAC Transparency	: off
Band Steering Mode	: disable
Band Steering Timeout(seconds)	: 5

publish-ssid

Enables broadcasting of an ESSID.

Syntax

publish-ssid
no publish-ssid

Command Mode

ESSID configuration

Default

An ESSID is broadcast by default.

Usage

When an ESSID is broadcast, it is included in the beacon that gets advertised. Clients using passive scanning listen for beacons transmitted by access points. If broadcasting an ESSID is disabled, clients listening for beacons cannot receive ESSID information.

Clients using active scanning send probe requests and wait for probe responses from access points. If broadcasting an ESSID is disabled, access points do not respond to probe requests, unless the probe request includes the ESSID.

Use the **no** form to prevent the ESSID from being broadcast.

Examples

The following disables the broadcasting of the ESSID named Eng:

```
controller# configure terminal
controller(config)# essid eng
controller(config-ssid)# no publish-ssid
controller(config-ssid)#
```

Related Commands

[ssid](#) on page 547

security-profile

Assigns a security profile, which defines security parameters, to the ESS.

Syntax

security-profile <*name*>

name Name of an existing security profile to be assigned to the ESS.

Command Mode

ESSID configuration

Default

The default security profile associated with an ESS is *default*.

Usage

Each ESS must be associated with a security profile. When you create an ESSID, it is automatically associated with a security profile named *default*. Use this command to assign a different security profile to an ESSID.

Before assigning a security profile to an ESS, you must first create the security profile using the **security-profile** command in global configuration mode.

Examples

The following command assigns the security profile *nms-group* to the ESSID named *eng*:

```
controller# configure terminal
controller(config)# ssid eng
controller(config-ssid)# security-profile nms-group
controller(config-ssid)#
```

Related Commands

- [ssid on page 547](#)
- [security-profile on page 467](#)

show ess-ap

Displays ESSID's and their associated access points.

Syntax

```
show ess-ap
show ess-ap <ap-id> <ssid> <Ifindex>
show ess-ap bssid <bssid>
show ess-ap channel <channel >
show ess-ap ssid <ssid> <ap-id> <Ifindex>
```

Command Mode

Privileged EXEC and ESSID configuration modes

Default

None

Usage

The output for the **show ess-ap** command differs depending on the its arguments and the command mode from which the command is entered. In privileged EXEC mode, all ESSID's and their associated access points are shown. In ESSID configuration mode, associated access points are shown for the ESSID being configured.

Examples

In privileged EXEC mode, the following command displays all ESSID's and their associated access points (the list is a partial display):

```
controller# show ess-ap
ESS Profile          AP ID AP Name          IfIndex Channel Max
Calls BSSID

mwf--1xtls          1    #1-2F-QA-208        2      161      0
00:0c:e6:69:4e:8c

mwf--1xtls          1    #1-2F-QA-208        1       1       0
00:0c:e6:14:40:f7

mwf--1xtls          2    #2-2F-Sw-208        2      161      0
00:0c:e6:69:4e:8c
controller#
```

Related Commands

[ess-ap](#) on page 546

show edited-bssid

Displays the BSSID table.

Syntax `show edited-bssid`

Command Mode Privileged EXEC

Default Disabled

Usage Use this command to view the list of configured edited-bssids.

Example

```
Asvin-test# show edited-bssid
AP ID IfIndex ESS Profile BSSID
11 1 Asvin_test 00:0c:e6:01:06:11
12 1 Asvin_test 00:0c:e6:01:06:12
      Edited Bssid Entry(2 entries)
Asvin-test#
```

Related Commands [edited-bssid](#) on page 545

Tunnel Interface Type	: none
VLAN Name	:
Virtual Interface Profile Name	:
GRE Tunnel Profile Name	:
Allow Multicast Flag	: off
Isolate Wireless To Wireless traffic	: off
Multicast-to-Unicast Conversion	: on
RF Virtualization Mode	: VirtualPort
Overflow from	:
APSD Support	: on
DTIM Period (number of beacons)	: 1
Dataplane Mode	: tunneled
AP VLAN Tag	: 0
AP VLAN Priority	: off
Countermeasure	: on
Multicast MAC Transparency	: off
Band Steering Mode	: disable
Band Steering Timeout(seconds)	: 5
Expedited Forward Override	: off
SSID Broadcast Preference	: till-association
B Supported Transmit Rates (Mbps)	: 1,2,5.5,11
B Base Transmit Rates (Mbps)	: 11
A Supported Transmit Rates (Mbps)	: 6,9,12,18,24,36,48,54
A Base Transmit Rates (Mbps)	: 6,12,24
G Supported Transmit Rates (Mbps)	: 6,9,12,18,24,36,48,54
G Base Transmit Rates (Mbps)	: 6,9,12,18,24,36,48,54
BG Supported Transmit Rates (Mbps)	:
1,2,5.5,11,6,9,12,18,24,36,48,54	
BG Base Transmit Rates (Mbps)	: 11
BGN Supported Transmit Rates (Mbps)	:
1,2,5.5,11,6,9,12,18,24,36,48,54	
BGN Base Transmit Rates (Mbps)	: 11
BGN Supported HT Transmit Rates (MCS)	:
0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23	
BGN Base HT Transmit Rates (MCS)	: none
AN Supported Transmit Rates (Mbps)	: 6,9,12,18,24,36,48,54
AN Base Transmit Rates (Mbps)	: 6,12,24

```
AN Supported HT Transmit Rates (MCS)      :  
0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23  
AN Base HT Transmit Rates (MCS)          : none  
Owner                                     : controller  
1 Stream VHT Base MCS Set (MCS)           : mcs0-9  
2 Streams VHT Base MCS Set (MCS)          : mcs0-9  
3 Streams VHT Base MCS Set (MCS)          : mcs0-9  
1 Stream VHT Supported MCS Set (MCS)      : mcs0-9  
2 Streams VHT Supported MCS Set (MCS)     : mcs0-9  
3 Streams VHT Supported MCS Set (MCS)     : mcs0-9  
InteropLab-MC1000#
```

**Related
Commands**

[essid](#) on page 547

ssid

Sets the SSID that is published over the air.

Syntax

ssid <ssid>

ssid Name of a unique SSID between 1 and 32 alphanumeric characters.

Command Mode

ESS configuration

Default

None

Usage

Use this command to set the SSID that is published over the air.



If you do not specify the SSID, it will default to the same name as the ESS profile.

Examples

Related Commands

- [essid](#) on page 547
- [show essid](#) on page 560

supported-tx-rates

Sets supported transmit rates in Mbps for a channel.

Syntax

```
supported-tx-rates 802.11a all
supported-tx-rates 802.11b all
supported-tx-rates 802.11g all
supported-tx-rates 802.11n all
supported-tx-rates 802.11bg all
supported-tx-rates 802.11bgn all
supported-tx-rates 802.11an all
supported-tx-rates 802.11an-mcs all
supported-tx-rates 802.11bgn-mcs all
supported-tx-rates 802.11a <Mbps rate>
supported-tx-rates 802.11b <Mbps rate>
supported-tx-rates 802.11g <Mbps rate>
supported-tx-rates 802.11n <Mbps rate>
supported-tx-rates 802.11bg <Mbps rate>
supported-tx-rates 802.11bgn <Mbps rate>
supported-tx-rates 802.11an <Mbps rate>
supported-tx-rates 802.11an-mcs <Mbps rate>
supported-tx-rates 802.11bgn-mcs <Mbps rate>
no supported-tx-rates (all variations shown above)
```

```
802.11b <Mbps rate>      1 | 2 | 5.5 | 11
802.11g <Mbps rate>      6 | 9 | 12 | 18 | 24 | 36 | 48 | 54
802.11bg <Mbps rate>     1 | 2 | 5.5 | 11 | 6 | 9 | 12 | 18 | 24 | 36 | 48 | 54
802.11bgn <Mbps rate>    1 | 2 | 5.5 | 11 | 6 | 9 | 12 | 18 | 24 | 36 | 48 | 54
802.11a <Mbps rate>      6 | 9 | 12 | 18 | 24 | 36 | 48 | 54
802.11an <Mbps rate>     6 | 9 | 12 | 18 | 24 | 36 | 48 | 54
802.11an-mcs <Mbps rate> 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15
802.11bgn-mcs <Mbps rate> 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15
```

Command Mode

ESS configuration

Default

```
802.11a base - 6,12,24 Mbps
802.11b base - 11 Mbps
```



```
802.11g base - 6,9,12,18,24,36,48,54 Mbps
802.11an base - 6,12,24 Mbps
802.11bg base - 11 Mbps
802.11bgn base - 11 Mbps
802.11an base - 6,12,24 Mbps
802.11an-ht-mcs base - none
802.11bgn-ht-mcs base - none
```

Usage

Setting the supported rate specifies the rates at which clients can optionally connect| provided the clients and the access points support the rate. Use the **no** form of the command to disable specified supported rates.

The supported data rates are the rates supported by the access points. The basic data rates are a subset of the supported rates. The access point first tries to transmit at the highest data rate set to Basic. If there are problems encountered in the transmission, the access points steps down to the highest rate that allows data transmission.

Examples

The following command sets the 802.11bg supported transmit rate to 11:

```
default(config-ssid)# supported-tx-rate 802.11bg 11
```

The following command sets the 802.11a supported transmit rate to support all rates (6, 9, 12, 18, 24, 36, 48, and 54 Mbps):

```
default(config-ssid)# supported-tx-rate 802.11a all
```

Related Commands

[base-tx-rates](#) on page 536

tunnel-type

Configures the type of tunnel that is being configured for the ESSID.

Syntax

```
tunnel-type GRE
tunnel-type configured-vlan-only
tunnel-type none
tunnel-type radius-and-configured-vlan
tunnel-type radius-only
```

Command Mode

ESSID configuration submode

Default

None

Usage

This command is used to specify a tunnel type, if a tunnel is being configured for the ESSID. A tunnel is specified for VLAN and GRE tunnel configurations, where a GRE configuration will always specify the GRE tunnel, and a VLAN can specify the remaining options (other than the type none).

Examples

To configure a GRE ESSID (which uses the same name as the GRE Profile), specify a tunnel-type GRE and security profile, as shown in the following example:

```
default# configure terminal
default(config)# essid guest
default(config-ssid)# tunnel-type GRE
default(config-ssid)# security-profile default
default(config)# exit
```

Related Commands

- [gre on page 342](#)
- [l2bridge appletalk on page 550](#)
- [ssid on page 547](#)
- [security-profile on page 557](#)
- [vlan on page 355](#)
- [vlan name on page 568](#)

virtual-port

Turns on Virtual Port, giving each client a unique connection to an AP300.

Syntax

```
virtual-port  
no virtual-port
```

Command Mode

Configuration mode

Default

None

Usage

When each client has its own Virtual Port, clients do not affect each other's performance. This command only applies if Virtual Cell mode is enabled.

Example

This example enables Virtual Cell, then enables Virtual Port on ESSID 5.

```
Master1# config terminal  
Master1(config)# interface Dot11Radio 239 1  
Master1(config-if-802)# virtual-cell-mode  
Master1(config-if-802)# exit  
Master1(config)# essid 5  
Master1(config-ssid)# virtual-port  
Master1(config-ssid)# exit
```

Related Commands

vlan name

Assigns a VLAN to an ESSID.

Syntax

```
vlan name <name>  
no vlan
```

Command Mode

ESSID configuration

Default

None

Usage

When creating an ESSID, you can assign a VLAN to the ESSID. This allows you to isolate an ESSID to a specific part of your network. By default, ESSIDs do not have VLANs assigned to them. You must create a VLAN using the **vlan** command in global configuration mode *before* assigning the VLAN name to an ESSID. As well, use the **tunnel-type** command to assign the tunnel-type of **configured vlan-only** or **radius-and-configured-vlan** to the ESSID.

Use the **no vlan** command to disable the VLAN assignment.

Examples

The following command assigns the *engineering* VLAN to an ESSID:

```
controller(config-ssid)# vlan name engineering  
controller(config-ssid)# tunnel-type configured-vlan-only
```

Related Commands

- [tunnel-type](#) on page 566
- [vlan](#) on page 355

wireless-to-wireless-isolation

Enables the ability to isolate traffic from individual stations connected to the same AP.

Syntax

```
wireless-to-wireless-isolation  
no wireless-to-wireless-isolation
```

Command Mode

ESSID configuration

Default

Disabled

Usage

In some wireless scenarios, it is necessary to ensure that two wireless stations belonging to the same L2 domain cannot communicate directly with each other. By enabling the **wireless-to-wireless-isolation** feature on an ESS, the two stations will be unable to communicate.

Use the **no wireless-to-wireless-isolation** command to disable this feature.

Examples

```
controller(config-ssid)# wireless-to-wireless-isolation  
controller(config-ssid)#
```

Related Commands

11

Access Point and Radio Commands

The commands contained in this chapter are used to configure and manage the connection between the controller and APs, as well as the AP radio settings. For many sites, default radio settings are adequate, but included are many commands that allow fine-tuning of the default radio settings for implementations with unique requirements.

- [*admin-mode*](#) on page 574
- [*antenna-gain*](#) on page 575
- [*antenna-property*](#) on page 576
- [*antenna-selection*](#) on page 577
- [*ap*](#) on page 578
- [*ap-keepalive-timeout*](#) on page 580
- [*ap-redirect*](#) on page 581
- [*auto-ap-upgrade*](#) on page 582
- [*autochannel*](#) on page 584
- [*boot-script*](#) on page 585
- [*building*](#) on page 586
- [*channel*](#) on page 587
- [*channel-width*](#) on page 589
- [*connectivity*](#) on page 590
- [*contact*](#) on page 592
- [*controller domainname*](#) on page 593
- [*controller hostname*](#) on page 594
- [*controller ip*](#) on page 595
- [*dataplane-encryption*](#) on page 596
- [*description*](#) on page 597
- [*fixed-channel*](#) on page 598
- [*floor*](#) on page 599
- [*hostname*](#) on page 600

- [interface Dot11Radio](#) on page 601
- [keepalive-timeout](#) on page 606
- [led](#) on page 603
- [link](#) on page 604
- [link-probing-duration](#) on page 605
- [localpower](#) on page 607
- [location](#) on page 609
- [mac-address](#) on page 610
- [mimo-mode](#) on page 611
- [mode](#) on page 613
- [model](#) on page 614
- [n-only-mode](#) on page 615
- [parent-ap](#) on page 616
- [power-supply](#) on page 618
- [preamble-short](#) on page 620
- [protection-mode](#) on page 622
- [protection-mode](#) on page 622
- [rfband](#) on page 623
- [rf-mode](#) on page 624
- [role](#) on page 625
- [show ap](#) on page 627
- [show ap-connectivity](#) on page 630
- [show ap-discovered](#) on page 632
- [show ap-redirect](#) on page 634
- [show ap-siblings](#) on page 629
- [show ap-swap](#) on page 635
- [show ess-ap](#) on page 636
- [show interfaces Dot11Radio](#) on page 637
- [show interfaces Dot11Radio antenna-property](#) on page 639
- [show interfaces Dot11Radio statistics](#) on page 642
- [show regulatory-domain](#) on page 647
- [show statistics ap300-diagnostics](#) on page 648
- [show statistics station-per-ap](#) on page 650
- [show statistics top10-ap-problem](#) on page 651

- *show statistics top10-ap-talker on page 653*
- *show topoap on page 655*
- *show topoapap on page 656*
- *swap ap on page 658*
- *type on page 661*

admin-mode

Manages radio interfaces.

Syntax

`admin-mode {Up | Down | Testing}`

Command Mode

Dot11Radio interface configuration

Default

The interface is Up by default.

Usage

This command allows control of whether an interface is enabled (**Up**) or disabled (**Down**). Setting the interface to **Down** makes the radio unavailable to client stations.

Throughput on dual-radio APs is slightly less than single radio APs due to the overhead of managing two radios. If the radio is not being used, it can be easily be temporarily disabled using this command to improve performance.

Examples

```
controller(config-if-802)# admin-mode Down
```

Related Commands

antenna-gain

Set the antenna band.

Syntax

antenna-gain {2.4GHz *gain*| 5GHz *gain*}

gain

Gain is an integer between 0 and 30.

Command Mode

Dot11Radio interface configuration

Default

Usage

Use this command to set the antenna gain to the type of radio in use with the command **rfband**.

Example

```
default# configure terminal
default(config)# interface Dot11Radio 10 1
default(config-if-802)# antenna-property 1
default(config-if-802-antenna)# antenna-gain 2.4GHz 8
default(config-if-802-antenna)# end
default(config-if-802)# end
default(config)# end
```

Related Commands

- [antenna-property](#) on page 576
- [interface Dot11Radio](#) on page 601

antenna-property

Manages external wireless antenna interface properties.

Syntax

antenna-property *connector*

connector Antenna connector ID; can be **1** (left antenna) or **2** (right antenna).

Command Mode

Dot11Radio interface configuration

Default

Usage

This command enters a subcommand mode that allows you to fine tune antenna properties such as gain and RF Band (2.4GHz, 5GHz or dual), and link type (point-to-point or point-to-multipoint).

Examples

```
controller(config-if-802)# antenna-property 1
```

Related Commands

- [antenna-gain](#) on page 575
- [antenna-selection](#) on page 577
- [interface Dot11Radio](#) on page 601
- [rfband](#) on page 623
- [show interfaces Dot11Radio antenna-property](#) on page 639
- [type](#) on page 661

antenna-selection

Configures the access point to use the left or right antenna.

Syntax

`antenna-selection {left | right | diversity}`

- | | |
|-----------|---|
| left | Configures the AP to use only the left antenna. |
| right | Configures the AP to use only the right antenna. |
| diversity | Configures an AP201 with 802.11b to use both antennas rather than just left or right. Using this feature allows the access point to receive from whichever antenna has the strongest signal.

The antenna must be set to “ left ” before using this command.

For proper functionality, the “ short-preamble ” feature must be off (default) to use the diversity mode. |

Command Mode

Dot11Radio interface configuration

Default

The default is for the system is to use the left antenna of an AP.

Usage

This command configures all access point models to use either the right or the left antenna. For the AP201 connected via 802.11b, **diversity** mode can be configured, which chooses the antenna receiving the stronger signal from the either the right or the left antenna.

Examples

```
controller(config-if_802)# antenna-selection right
controller(config-if_802)#
```

Related Commands

[antenna-property](#) on page 576

ap

Enters access point configuration.

Syntax

ap *id*
no ap *id*

id The unique identifier for the access point.

Command Mode

Global configuration

Default

None

Usage

Use the **ap** command with an identifying number to enter the AP configuration submode to configure that particular access point. Use the **no ap id** command to remove a Controller-to-AP assignment.

Examples

```
controller(config)# ap 1
controller(config-ap)# ?
boot-script          Configure boot script for this AP.
building             Building location for this AP.
connectivity         Manage AP connectivity.
contact              Contact person for this AP.
dataplane-mode       Determine whether the data packets go through the
controller or not.
default              Reset to default values
description           Description of AP.
do                   Executes an IOSCLI command.
end                  Save changes, and return to privileged EXEC mode.
exit                 Save changes, and return to global configuration
mode.
floor                Floor location for this AP.
led                  Configure LED settings.
link-probing-duration Duration AP waits before rebooting when controller
link is down.
```

location	Location of this AP.
mac-address	Assign a new MAC address or pre-provision AP.
model	Assign AP HW type.
no	Disables various parameters.
show	Displays parameters related to this AP.

Related Commands

- [boot-script](#) on page 585
- [building](#) on page 586
- [contact](#) on page 592
- [connectivity](#) on page 590
- [description](#) on page 597
- [floor](#) on page 599
- [hostname](#) on page 600
- [led](#) on page 603
- [link-probing-duration](#) on page 605
- [location](#) on page 609
- [mac-address](#) on page 610

ap-keepalive-timeout

Configures AP keepalive timeout in seconds.

Syntax

ap-keepalive-timeout <value>

value Enter the AP keepalive timeout in seconds (1-1800)

Command Mode

Global configuration

Default

None

Usage

Examples

```
controller# configure terminal
controller(config)# ap-keepalive-timeout 10
```

Related Commands

ap-redirect

Redirects APs to another controller.

Syntax

```
ap-redirect ip-subnet <ip_addr subnet_addr> <controller_ip_addr>  
ap-redirect ip-subnet mac-address <MAC_addr> <controller_ip_addr>  
no ap-redirect
```

ip-subnet ip_addr sub-net_addr	Specifies the IP or subnet address of one or more APs that are to be redirected.
mac-address mac_addr	Specifies the MAC address of the AP to be redirected.
controller_ip_addr	Specifies the Controller hostname or IP address where APs are to be redirected.

Command Mode

Global configuration

Default

None

Usage

This command allows you to specify APs (by MAC address or by IP subnet address) that are to be redirected to another controller (specified by its hostname or IP address). Redirection takes place after initial discovery. Each controller can have a redirect table that associates the AP's MAC/IP subnet address to an IP address or hostname of a controller. A maximum of 5 hops (redirects) are allowed per AP.

Use the **no** form of the command to remove a redirection assignment.

Examples

```
controller(config-ap)# ap-redirect mac-address 00:0c:e6:00:01:02  
172.10.10.5  
controller(config-ap)#
```

Related Commands

[show ap-redirect](#) on page 634

auto-ap-upgrade

Allows AP firmware to be automatically upgraded by the controller.

Syntax

```
auto-ap-upgrade {enable | disable}
```

enable	Activates the AP automatic upgrade feature. This is the default setting.
--------	--

disable	Deactivates the AP automatic upgrade feature.
---------	---

Command Mode

Global configuration

Default

The AP automatic upgrade feature is enabled by default.

Usage

This command allows the firmware on an AP to be automatically upgraded by the controller when an AP joins the WLAN. An AP cannot be monitored (and consequently, be part of the WLAN) if its firmware is at a different level than that of the controller.

When an AP initiates its discovery phase, the controller checks the firmware version and performs an upgrade if the version is not at the same level as that of the controller. This feature simplifies the process of adding a group of APs to an existing WLAN.

When this feature is enabled, you can check the upgrade status of affected APs through syslog messages and SNMP traps that warn of an AP/controller software version mismatch. An alarm is dispatched to an SNMP manager if a mismatch exists, meaning the AP is unable to upgrade for some reason. Once the upgrade is performed, syslog and SNMP traps are sent notifying of the AP/controller software version match. Alarms must be cleared manually.

This feature does not interfere with a normal WLAN system upgrade when the **upgrade** command is used.

Examples

```
controller(config)# auto-ap-upgrade enable
```

```
controller# show controller
Global Controller Parameters
```

Controller ID : 1

Description	: 3dot4dot1 Controller
Host Name	: forti-ess
Uptime	: 03d:01h:17m:33s
Location	: Qa scale testbed
near IT	
room	
Contact	: Raju
Operational State	: Enabled
Availability Status	: Online
Alarm State	: No Alarm
Automatic AP Upgrade	: on
Virtual IP Address	: 192.168.9.3
Virtual Netmask	: 255.255.255.0
Default Gateway	: 192.168.9.1
DHCP Server	: 10.0.0.10
Statistics Polling Period (seconds)/0 disable Polling	: 60
Audit Polling Period (seconds)/0 disable Polling	: 60
Software Version	: 4.1-48
Network Device Id	: 00:90:0b:07:9f:6a
System Id	: 245AA7436A21
Default AP Init Script	:
DHCP Relay Passthrough	: on
Controller Model	: MC3000
Country Setting	: United States Of
America	
Manufacturing Serial #	: N/A
Management by wireless stations	: on
Controller Index	: 0

autochannel

Performs automatic channel configuration.

Syntax

autochannel *channel_list*

channel_list A list of 802.11bg and/or 802.11a channels separated by white space. An appropriate channel for the type of wireless interface will automatically be applied.

Command Mode

Global configuration

Default

None

Usage

This command automatically assigns channels to APs.

When **autochannel** runs, it checks that the channels specified as arguments are valid for the AP's configured country code. If a channel is invalid, it displays an error message specifying the valid list of channels. The optimum channel is then selected and set for the specific AP interface (based on the RF band that is configured for that interface, b/g or a). The process takes approximately 2 minutes, during which time the APs are not operational.

To exclude an interface from an autochannel assignment, use the **channel** and **fixed-channel** commands.

Examples

```
controller(config)# autochannel 2 3 4
```

Pre-initialization:

out of 44 APs, 3 are enabled

Related Commands

- [channel](#) on page 587
- [fixed-channel](#) on page 598

boot-script

Runs a specified script when an access point boots.

Syntax

```
boot-script script  
no boot-script
```

script Name of the script to run.

Command Mode

Global configuration

Default

None

Usage

Use this command to boot the access point with a specific script. You can see a list of available scripts with the **show ap scripts** command from the *privileged exec* command mode.

Use the **no** form of the command to disable the default AP boot script.

Examples

```
controller# show scripts  
default  
debug  
cli  
controller# configure terminal  
controller(config)# boot-script default  
controller(config)
```

Related Commands

[boot-script](#) on page 585

building

Specifies the building in which an access point is located.

Syntax

building *building-name*

building-name Name of the building in which the access point is located. The building name can be up to 64 alphanumeric characters long. To use spaces in the name, enclose the name in double quotation marks (" ").

Command Mode

Access point configuration

Default

None

Usage

Using the **building** command is optional and is only used for informational purposes.

Examples

The following commands specify that an access point with a node ID of 2 is located in building 1:

```
controller# ap 2
controller(config-ap)# building "building 1"
controller(config-ap)# exit
```

Related Commands

- [floor](#) on page 599
- [location](#) on page 609

channel

Sets the channel number for the wireless interface to use.

Syntax

channel *channel*

channel Channel ID

Command Mode

Dot11Radio interface configuration

Default

None

Usage

Sets the wireless interface channel. Typing **channel ?** lists the available channels for the type of radio in use.

To ensure the channel set is not changed if the **autochannel** command is run, use the **fixed-channel** command.

Examples

```
controller(config-if_802)# channel ?
<channel>                      Enter the channel ID.
 1
10
11
149
153
157
161
165
 2
 3
36
 4
40
44
```

48

5

52

56

6

60

64

7

8

```
controller(config-if_802)# channel 149
```

Related Commands

- [*autochannel*](#) *on page 584*
- [*fixed-channel*](#) *on page 598*

channel-width

Changes AP300 channel width.

Syntax

channel-width [20-mhz | 40-mhz-extension-channel-above | 40-mhz-extension-channel-below]

20-mhz	Sets channel width to 20 MHz
40-mhz-extension-channel-above	Sets channel width to 40 MHz by bonding with the extension channel above it
40-mhz-extension-channel-below	Sets channel width to 40 MHz by bonding with the extension channel below it

Command Mode

Interface Dot11Radio configuration submode

Default

20 MHz

Usage

Use this command to change the channel width from 20 MHz (default) to 40 MHz (either 40-mhz-extension-channel-above or 0-mhz-extension-channel-below 40) . This command also sets channel bonding to create 40 MHz.

Examples

The following command increases the channel width of an AP to 40 MHz by channel bonding with the channel above it:

```
default config terminal
default(config)interface Dot11Radio 1 1
default(config-if-802)# channel-width-above-40-MHz-Extension-channel
```

The following channel-width command increases the channel width of an AP to 40 MHz by channel bonding with the channel below it:

```
default config terminal
default(config)interface Dot11Radio 1 1
default(config-if-802)# channel-width below-40-MHz-Extension-channel
```

connectivity

Manages AP connectivity and puts you into AP connectivity mode if using **l2-preferred** or **l3-preferred**.

Syntax

`connectivity { l2-only / l2-preferred / l3-preferred }`

l2-only	Uses Layer 2 only for AP discovery.
l2-preferred	Uses Layer 2 as first attempt for AP discovery. If a controller is not found within 16 seconds, it then attempts Layer 3 discovery.
l3-preferred	Uses Layer 3 as first attempt for AP discovery. If a controller is not found within 16 seconds, it then attempts Layer 2 discovery.

Command Mode

AP configuration

Default

The default connectivity is Layer 2 preferred.

Usage

This command is used to manage the connectivity of an AP to a controller. The AP and controller can be in the same subnet or they can be in different subnets, separated by one or more routers.

When an AP joins a WLAN, it searches for a controller to link to. By default, the AP uses Layer 2 MAC address broadcast discovery packets to allow it to be found by a controller. When the controller and AP are in the same subnet, the AP is discovered by the controller and configuration information is downloaded from the controller to the AP.

As the Layer 2 protocol does not allow the discovery packets outside of the subnet, if the controller is not in the same subnet as the AP, Layer 3 routing must be established. The default connectivity switches to Layer 3 discovery if a controller is not found within 16 seconds.

If the configuration uses a router between subnets, and the AP is in a different subnet than the controller, use the **l3-preferred** option to initiate Layer 3 connectivity to the controller. In this configuration, if a DNS server is set up to contain the default name of the controller, "wlan-controller," with the controller IP address "default," a connection between the AP and controller can automatically be established and the AP can receive its configuration information from the controller.

Choose **l2-preferred** or **l3-preferred** to enter into **ap-connectivity** mode. In this mode, a controller IP address, hostname, and domain name can be explicitly configured.



If you have APs configured for L3 preferred discovery and you change the IP address of the controller, the configuration of all APs need to be updated with the new IP address of the controller, or the APs will not find the controller on reboot. If your AP cannot find the controller, you can reconfigure it by moving the AP onto the same L2 subnet as the controller and after several minutes of failed L3 discovery it will revert to L2 broadcast discovery, after which the IP of the controller can be reconfigured to the new value.

Examples

The following commands can be used to setup a Layer 3 configuration for an AP not in the same subnet as the controller. The first command enters connectivity mode, then configures the AP to obtain its IP address from DHCP (which then allows the AP to connect the DNS server and query for the IP address for the hostname “wlan-controller”):

```
controller(config-ap)# connectivity l3-preferred
controller(config-ap-connectivity)#ip address dhcp
controller(config-ap-connectivity)#controller hostname wlan-controller
```

Related Commands

- [controller domainname on page 593](#)
- [controller hostname on page 594](#)
- [controller ip on page 595](#)
- [ip address dhcp on page 268](#)
- [ip dns-server on page 273](#)
- [show ap-connectivity on page 630](#)

contact

Provides the contact person for the access point.

Syntax

contact *contact*

contact Contact name

Command Mode

AP configuration

Default

None

Usage

This command sets the contact person for the access point.

Examples

```
controller(config-ap)# contact Bob
controller(config-ap)#
```

Related Commands

[location](#) on page 609

controller domainname

Configures the controller domain name from where the access point is discovered.

Syntax

`controller domainname`

Command Mode

AP connectivity configuration

Default

None

Usage

Configures the controller's domain name.

Examples

```
controller(config-ap-connectivity)# controller domainname acme
controller(config-ap-connectivity)#
```

Related Commands

- [controller hostname on page 594](#)
- [controller ip on page 595](#)

controller hostname

Configures the controller hostname from where the access point is discovered.

Syntax

`controller hostname hostname`

Command Mode

AP connectivity configuration

Default

None

Usage

Configures the controller's IP hostname.

Examples

```
controller(config-ap-connectivity)# controller hostname acmeCorp
controller(config-ap-connectivity)#
```

Related Commands

- [controller domainname](#) on page 593
- [controller ip](#) on page 595

controller ip

Configures the controller IP from where the access point is discovered.

Syntax

controller ip *address*

address Sets the controller IP address

Command Mode

AP connectivity configuration

Default

None

Usage

Configures the controller's IP address.

Examples

```
controller(config-ap-connectivity)# controller ip address 10.0.220.30  
controller(config-ap)#
```

Related Commands

- [controller domainname](#) on page 593
- [controller hostname](#) on page 594

dataplane-encryption

Enables and disables encryption on the dataplane connection between AP and controller.

Syntax `dataplane-encryption {on | off}`

Command Mode AP configuration

Default Dataplane encryption is off

Usage This command encrypts the dataplane connection between the AP and the controller. It was designed for use with Mesh and Remote AP, but can be used elsewhere. This feature provides an IPsec-like security mode where the data traffic sent over the data tunnel is encrypted by the AP and controller (at their endpoints). The encryption algorithm is 3DES. Note that enabling this feature affects performance because the encryption/decryption is done with software.

Examples

```
controller(config-ap)# dataplane-encryption on
controller(config-ap)#
```

Related Commands

| description

A text description for the access point.

Syntax	<div><div><code>description</code></div><div><i>description</i></div></div>
	<div><div><i>description</i></div><div>Description of the access point. Descriptions longer than 64 characters may impact readability on the Web interface page.</div></div>
Command Mode	AP configuration
Default	None
Usage	Describes the access point in text.
Examples	<pre>controller(config-ap)# description serves_QA+IT controller(config-ap)#</pre>
Related Commands	<ul style="list-style-type: none">• building on page 586• floor on page 599• location on page 609

fixed-channel

Fixes the RF channel so it cannot be changed by autochannel configuration.

Syntax

```
fixed-channel enable  
no fixed-channel
```

enable Enables fixed-channel mode.

Command Mode

Dot11Radio interface configuration

Default

No fixed-channel

Usage

This command is used to prevent the autochannel assignment performed with the **auto-channel** command. Use the **enable** keyword to activate fixed-channel functionality. Use the **channel** command to set the channel, prior to fixing the channel, with this command.

Use the **no fixed-channel** command to return to autochannel mode.

Examples

```
controller(config-if_802)# fixed-channel enable  
controller(config-if_802)#
```

Related Commands

- [autochannel](#) on page 584
- [channel](#) on page 587

floor

Specifies the floor on which an access point is located.

Syntax

floor *floor-name*

floor-name Name of the floor on which the access point is located. The floor name can be up to 64 alphanumeric characters long. To use spaces in the name, enclose the name in double quotation marks (" ").

Command Mode

Privileged EXEC

Default

None

Usage

Using the **floor** command is optional and is only used for informational purposes.

Examples

The following commands specify that an access point with the node ID of 2 is located on the second floor:

```
controller# ap 2
controller(config-ap)# floor "second floor"
controller(config-ap)#
```

Related Commands

- [building](#) on page 586
- [location](#) on page 609

hostname

Sets the access point hostname.

Syntax

hostname *hostname*

hostname

Hostname from 1-37 characters.

Command Mode

AP connectivity configuration

Default

None

Usage

Sets the access point hostname.

Examples

```
controller(config-ap)# hostname acme  
controller(config-ap)#
```

interface Dot11Radio

Selects AP radio interface for configuration and enters 802.11 configuration mode.

Syntax

interface Dot11Radio *node-id interface_ID*

<i>node-id</i>	Selects the access point to configure
<i>interface_ID</i>	Specifies the first or the second radio interface, if two radios are present on the AP. <i>interface_ID</i> can be 1 or 2.

Command Mode

Global configuration

Default

None

Usage

Puts you in Dot11Radio mode for configuring individual access point interfaces.

Examples

```
controller(config)# interface Dot11Radio 1 1
controller(config-if-802)# ?
admin-mode           Administrative Mode.
antenna-property     Manage external wireless interface antennas.
antenna-selection    Antenna configuration.
channel              Configure the channel ID.
default              Set various parameters to the default value.
do                   Executes an IOSCLI command.
end                  Save changes, and return to privileged EXEC mode.
exit                 Save changes, and return to global configuration
mode.
fixed-channel         Fix channel so it cannot be changed by auto-channel
configuration.
interop-mode         B/G protection mechanism.
mode                 AP mode configuration.
no                   Disables various parameters.
```

power example, 20,20,20.	Transmit power in the format low,medium,high. For
preamble-short	Enables short preamble.
protection-mode	bg protection mode.
rf-mode or bg).	Configure the Radio Frequency mode (802.11a, b, g,
scanning-channels	Configure the channels for scanning.
show interface.	Displays various parameters related to this wireless
tuning	Tune wireless interface.

Related Commands

- [antenna-property](#) on page 576
- [antenna-selection](#) on page 577
- [channel](#) on page 587
- [fixed-channel](#) on page 598
- [protection-mode](#) on page 622
- [preamble-short](#) on page 620

led

Specifies the blinking pattern of the LED Mode light.

Syntax

```
led {blink | NodeId | Normal}
```

blink	LED Mode blinks two short blinks followed by four short blinks
NodeId	The LED Mode light blinks short green blinks indicating the last digit of the AP ID. The number of short green lights is equal to the number of the AP ID modulo 10. Therefore, for AP IDs 4, 14, and 24, the NodeID mode blinks with a long yellow light followed by 4 short green lights. For AP IDs 7, 17, and 27, the NodeID mode blinks with a long yellow light followed by 7 green lights. Using this mode helps you identify the AP from other APs in the system.
Normal	The LED blink pattern is controlled by the AP.

Command Mode

AP configuration

Default

The default is **blink** (blinking).

Usage

Use this command to specify the blinking pattern of the LED Mode light. When there is no activity in either case, the LED is off/not illuminated.

Examples

The following command changes the blinking pattern to **Normal**:

```
controller(config-ap)# led normal
```

link

Specifies the link type for an AP connector.

Syntax

`link {Point-To-Point | Point-To-Multi-Point}`

Command Mode

Antenna Properties submode configuration

Default

Point-To-Multi-Point

Usage

Specifies the type of link for the connector.

Examples

`controller(config-ap)# link Point-To-Point`

Related Commands

- [antenna-property](#) on page 576
- [ap](#) on page 578

link-probing-duration

Specifies the duration an AP waits before rebooting when controller link is broken.

Syntax

`link-probing-duration duration`

duration

Specifies the AP wait duration in minutes. *duration* can be from 1 to 32000.

Command Mode

AP configuration

Default

None

Usage

Specifies the duration of time (from 1 to 32000 minutes), that bridged APs wait before rebooting when the controller link is broken. This command is used in Remote AP configurations to prevent AP reboots when the connectivity to the remote controller is lost.

Examples

```
controller(config-ap)# link-probing-duration 32000
```

Related Commands

keepalive-timeout

Specifies the duration of time (from 1 to 1800 seconds), for the remote APs to remain in the online state with respect to the controller, even when the link to the AP is down.

Syntax

`controller(config-ap)# keepalive-timeout 1800`

Command Mode

AP configuration

Default

None

Usage

Specifies the duration of time (from 1 to 1800 seconds), for the remote APs to remain in the online state with respect to the controller, even when the link to the AP is down.

Examples

`controller(config-ap)# keepalive-timeout 1800`

Related Commands

localpower

Configures the AP radio maximum transmit power, including antenna gain.

Syntax

`localpower power-level`

power-level The transmit power level (dBm) for the radio. This level is dependant upon the radio band and country code in use. In the United States, the *power-level* can be an integer between:

- **5** to Max/channel (see table below) for 802.11a radios
- **4** to **30** for 802.11/b/g radios

Command Mode

Dot11Radio interface configuration

Default

20 for 802.11/b/g radios; 17 for 802.11a radios

Usage

Transmit power in Fortinet's terminology is the EIRP1 (Effective Isotropic Radiated Power) at the antenna and includes the antenna gain. (This is important to remember; transmit power is not the power at the connector.) The radio transmit power setting helps manage contention between neighboring access points. Power level settings are dependent on the country code and the radio band (and for 802.11a, the channel) in use.

The following table shows channels and maximum power for the United States:

Channel	Maximum Transmit Power (dBm) for USA
36	23
40	23
44	23
48	23
52	30

Channel	Maximum Transmit Power (dBm) for USA
56	30
60	30
64	30
100	30
104	30
108	30
112	30
116	30
120	30
124	30
128	30
132	30
136	30
140	30
149	36
153	36
157	36
161	36
165	36

Examples

The following lowers the power level for an 802.11/bg radio:

```
controller(config-if_802)# localpower 17
controller(config-if_802)#
```

location

The location of the access point.

Syntax

location *Location*

location Location of the access point.

Command Mode

AP configuration

Default

None

Usage

Describes the location of the access point.

Examples

```
controller(config-ap)# location 10ft_from_west_window
```

Related Commands

- [contact](#) on page 592
- [description](#) on page 597

mac-address

The MAC address of the access point.

Syntax

mac-address <*MAC-address*>

mac-address MAC address of the access point in hexadecimal format.

Command Mode

AP configuration

Default

None

Usage

Configures the MAC address for the access point.

Examples

```
controller(config-ap)# mac-address 00:E5:F0:B8:2A:3F00:12:F2:B8:2A:3F
controller(config-ap)#
```

Related Commands

[ap](#) on page 578

mimo-mode

Configures the MIMO mode on an AP300.

Syntax

mimo-mode [2x2 | 3x3]

- 2x2 Send two streams of data and receive data in two streams on this AP.
- 3x3 Send three streams of data and receive data in three streams on this AP.

Command Mode

Interface Dot11Radio configuration submenu

Default

2x2

Usage

Use this command to set MIMO Mode on an AP300. MIMO Mode must be coordinated with the AP300 power supply setting. The relationship between MIMO Mode and power supply is shown in the chart below.

Power Supply	Supports this MIMO Mode
802.3-af	Default power supply. Select when using a traditional 802.3-af PoE. This power supply type only supports 2x2 MIMO mode on the AP300.
802.3-at	Select when using a higher-powered, next generation PoE. This power supply type supports both 2x2 and 3x3 MIMO modes on the AP300.
5V-DC	Select when an optional ACC-AP300-PWR power supply is plugged into a wall outlet. This power supply type supports both 2x2 and 3x3 MIMO modes.
dual-802.3af	Select when using a dongle that combines power from two traditional 802.3-af PoEs. This power supply type supports both 2x2 and 3x3 MIMO mode.

Examples

The following mimo-mode command sets MIMO Mode to 3x3:

```
default config terminal
default(config)interface Dot11Radio 1 1
default(config-if-802)# mimo-mode 3x3
```

Related Commands

power-supply on page 618

mode

Configures the AP radio mode to monitor-only or provide normal wireless service.

Syntax

`mode {normal | scanning}`

normal Sets the AP radio to provide normal wireless services.

scanning Sets the AP radio to provide only continuous monitoring service.

Command Mode

Dot11Radio interface configuration

Default

Usage

Configures the specified access point's radio to provide the specified service type. For the AP200 with two radios installed, allows you to configure the functionality mode of each radio.

Examples

```
controller(config-if_802)# mode scanning
controller(config-if_802)#
```

model

Configures the AP model type.

Syntax

model {*type*}

type Sets the AP model type.

Command Mode

AP configuration

Default

Usage

Configures the specified Access Point hardware model type.

Examples

```
controller(config-ap)# model AP320  
controller(config-ap)#
```

n-only-mode

Enables/disables 802.11n-only on a radio for APs supporting 802.11n.

Syntax

n-only-mode
no n-only-mode

Command Mode

Dot11Radio submode

Default

802.11n only mode is disabled.

Limitations

Not supported on non-802.11n APs.

Usage

On APs that support 802.11n, use the **n-only-mode** command to enable only the 802.11n protocol on that radio and allow only 802.11n clients to associate. This improves performance, as sharing the radio with clients for 802.11bg or 802.11a (depending on the frequency band) slows down the 802.11n throughput.

Use the **no n-only-mode** command to disable this mode and allow 802.11bg or 802.11a users to associate.

Examples

To enable this feature on the radio:

```
controller(config-if-802)# n-only-mode
```

To disable this feature on the radio:

```
controller(config-if-802)# no n-only-mode
```

Related Commands

[*show interfaces Dot11Radio*](#) on page 637

parent-ap

For Enterprise Mesh, configures the ID of the Parent AP.

Syntax

parent-ap **AP_ID**

ID An integer that represents the Parent AP.

Command Mode

AP configuration

Default

The Parent AP ID is set to 0.

Usage

For the Enterprise Mesh configuration, the Parent AP is the AP that is designated to provide a backhaul connection for the AP being configured. The Parent AP is configured for wireless mode APs; it is not configured on the gateway AP.

In the Enterprise Mesh configuration, only the first tier, the gateway AP, is connected via a wired Ethernet connection. The remaining APs in the mesh are either an intermediate or leaf AP, which use their 802.11a channel for backhaul wireless communication with the Parent AP.

See the “Enterprise Mesh” chapter of the FortiWLC (SD) Configuration Guide for a complete description of this feature, including configuration steps.

Examples

The following example sets the AP 1 as the Parent AP for AP 2.

```
controller(config-ap)# parent-ap 1
controller(config-ap)#
```

The Parent AP setting is shown with the show ap command:

```
controller(config-ap)# do show ap 2
AP Table
```

AP ID	: 2
AP Name	: AP-2
Serial Number	: 00:12:F2:00:00:24

Uptime	: 00d:00h:00m:00s
Location	:
Building	:
Floor	:
Contact	:
Operational State	: Enabled
Availability Status	: Online
Alarm State	: No Alarm
LED Mode	: Normal
AP Init Script	:
Boot Image Version	: 3.9
FPGA Version	: wmac0:14.0
Runtime Image Version	: 3.5-46
Connectivity Layer	: None
Dataplane Encryption	: off
AP Role	: wireless
Parent MAC Address	: 00:12:F2:00:00:23
Parent AP ID	: 1
Link Probing Duration	: 120
AP Model	: AP100
AP Label	: ATS1
Sensor AP ID	: 0
Hardware Revision	: Rev 3

Related Commands

- [ap](#) on page 578
- [role](#) on page 625
- [show ap](#) on page 627

power-supply

Directs the AP300 to seek power from the named source.

Syntax

`power-supply [5V-DC | 802.3-af | 802.3-at | dual-802.3-af]`

Power Supply	Supports this MIMO Mode
802.3-af	Default power supply. Select when using a traditional 802.3-af PoE. This power supply type only supports 2x2 MIMO mode on the AP300.
802.3-at	Select when using a higher-powered, next generation PoE. This power supply type supports both 2x2 and 3x3 MIMO mode on the AP300.
5V-DC	Select when an optional ACC-AP300-PWR power supply is plugged into a wall outlet. This power supply type supports both 2x2 and 3x3 MIMO mode.
dual-802.3-af	Select when using a dongle that combines power from two traditional 802.3-af PoEs. This power supply type supports both 2x2 and 3x3 MIMO mode.

Command Mode

AP configuration submode

Default

5V-DC

Usage

Use this command to set the power supply for an AP300.

Be sure to change the power supply setting to either **DC power supply** or **802.3at PoE** before changing MIMO mode to 3x3.

Examples

The following command directs an AP300 to seek power from a wall outlet power supply:

```
default config terminal
default(config)ap 1
default (config-ap)# power-supply 5V DC
```

Related Commands

mimo-mode on page 611

preamble-short

Indicates whether short preamble is used.

Syntax

```
preamble-short  
no preamble-short
```

Command Mode

Dot11Radio interface configuration

Default

The short preamble is set by default.

Usage

Use this command to set a preamble. Use the **no** feature to disable short and use a long preamble. This feature is either on or off.

Examples

```
controller(config-if_802)# preamble-short  
controller(config-if_802)#
```

Related Commands

protection-cts-mode

Configures the radio interoperability mode.

Syntax

protection-cts-mode {wmm-txop | 802.11-1999}

wmm-txop	WMM-style TXOP protection for 802.11g frames. Improves performance of 802.11g clients above typical throughput in a mixed 802.11b/802.11g environment.
802.11-1999	One frame protection for 802.11g frames.Provides standard 802.11 mixed 802.11b/802.11g performance.

Command Mode

Dot11Radio interface configuration

Default

The default mode is 802.11-1999.

Usage

Configures the access point's interoperability mode. The wmm-txop option uses the WMM TXOP feature in an intelligent manner for data to provide performance gains.

Examples

```
controller(config-if_802)# protection-cts-mode wmm-txop
```

| protection-mode

Manages bg protection mode settings.

Syntax

```
protection-mode {auto | off | on}
no protection-mode
```

auto	Dual-speed protection mode is automatically enabled for the type of radio in use.
off	Dual-speed protection mode is always disabled.
on	Dual-speed protection mode is always enabled.

Command Mode

Dot11Radio interface configuration

Default

The protection mode **auto** setting is enabled by default.

Usage

Use this command to set the bg mixed-mode protection mechanism mode for the radio interface to **on**, **off**, or **automatic**. If **auto** is selected, 802.11bg Dual-Speed protection mechanism is enabled for the type of radio in use. For 802.11bg radios, optimal performance for 802.11g clients is achieved if 802.11b clients are present and the protection mode is enabled (**on** or **auto**). This option has no impact for 802.11b only or 802.11a radios.

Examples

To disable the automatic protection mode settings:

```
controller(config-if_802)# protection-mode off
```

To enable the protection mode settings:

```
controller(config-if_802)# protection-mode on
```

To set the protection mode settings back to automatic:

```
controller(config-if_802)# protection-mode auto
```

Related Commands

[*rf-mode*](#) on page 624

rfband

Set the antenna band.

Syntax

`rfband {2.4GHz | 5GHz | dual}`

Command Mode

Dot11Radio interface configuration

Default

Usage

When configuring dual band radio operation, set the antenna band to the type of radio in use with the command **rfband**.

Example

```
default# configure terminal
default(config)# interface Dot11Radio 10 1
default(config-if-802)# antenna-property 1
default(config-if-802-antenna)# type External-dual-mode
default(config-if-802-antenna)# rfband dual
default(config-if-802-antenna)# end
default(config-if-802)# end
default(config)# end
```

Related Commands

- [antenna-property](#) on page 576
- [antenna-selection](#) on page 577
- [interface Dot11Radio](#) on page 601

rf-mode

Configures the radio frequency mode.

Syntax

rf-mode *mode*

mode

Specifies the radio frequency. *mode* can be:

- **802.11a**—Specifies the 802.11a standard.
- **802.11b**—Specifies the 802.11b standard.
- **802.11bg**—Specifies the 802.11b/g interop mode.
- **802.11g**—Specifies the 802.11g standard.

Command Mode

Dot11Radio interface configuration

Default

Usage

Configures the access point's radio frequency mode. This command allows you to choose the radio band. When the 802.11bg mode is selected, you can also configure the proprietary protection mode that improves performance for g clients in a bg mixed environment.

Examples

On an AP 201, choose to implement the 802.11bg mixed mode with the command:

```
controller(config-if_802)# rf-mode 802.11bg
controller(config-if_802)#
```

Related Commands

[*protection-mode*](#) **on page 622**

role

Configures the operational role the AP in the WLAN.

Syntax

```
role { access | gateway | wireless }
```

access	The role of the AP in a non-Enterprise Mesh configuration (default).
gateway	In Enterprise Mesh configurations, the AP that is connected via the Ethernet port.
wireless	In Enterprise Mesh configurations, any AP that is not the gateway AP.

Command Mode

AP configuration

Default

access mode

Usage

An AP is in one of the three modes: access, gateway, or wireless. APs that are not part of an Enterprise Mesh are in access mode.

For the Enterprise Mesh configuration, the one AP is designated the gateway AP and all others are in wireless mode.

In the Enterprise Mesh configuration, only the first tier, the gateway AP, is connected via a wired Ethernet connection. The remaining APs in the mesh are either an intermediate or leaf AP, all of which are wireless. Wireless APs use their 802.11a channel for backhaul wireless communication with the Parent AP.

See the “Enterprise Mesh” chapter of the FortiWLC (SD) Configuration Guide for a complete description of this feature, including configuration steps.

Examples

The following example sets the AP 1 as the gateway AP:

```
controller(config-ap)# role gateway
controller(config-ap)#
```

The Parent AP setting is shown with the show ap command:

```
controller(config-ap)# do show ap 1
AP Table
```

AP ID	: 1
AP Name	: AP-1
Serial Number	: 00:12:F2:00:00:23
Uptime	: 00d:00h:00m:00s
Location	:
Building	:
Floor	:
Contact	:
Operational State	: Disabled
Availability Status	: Offline
Alarm State	: No Alarm
LED Mode	: Normal
AP Init Script	:
Boot Image Version	: 3.9
FPGA Version	: wmac0:14.0
Runtime Image Version	: 3.5-46
Connectivity Layer	: None
Dataplane Encryption	: off
AP Role	: gateway
Parent MAC Address	: 00:00:00:00:00:00
Parent AP ID	: 0
Link Probing Duration	: 120
AP Model	: AP100
AP Label	: ATS1
Sensor AP ID	: 0
Hardware Revision	: Rev 3

Related Commands

- [*ap*](#) on page 578
- [*parent-ap*](#) on page 616
- [*show ap*](#) on page 627

show ap

Displays information about the access point

Syntax

`show ap [node-id]`

node-id Optional. The identification number of the access point

Command Mode

EXEC

Default

None

Usage

Displays access point information, including AP ID and name, MAC address, operational state, availability status, runtime image version, connectivity layer, model type, and remote/local placement. Enter an optional ID to see detailed information about one access point. Do not enter any ID to see high-level information about all access points currently on the system.

Use the operational state and availability status to assess the state of the access point. The most common combinations and their meaning are:

- Enabled and On-line: Access point is operating correctly.
- Disabled and Off-line: Controller cannot communicate with the access point.
- Disabled and On-line: Access point or network is not configured correctly.

The availability status is used to monitor is a piece of equipment has been pre-provisioned, discovered, or simply powered off. All possible values for this state are included in the following table:

Availability Status	Description
Not Installed	The network element has been pre-provisioned, but not yet discovered
PowerOff	The network element is installed (has been discovered at least once), but it is not currently powered on.

Availability Status	Description
Off-line	The network element is powered-on, but it has been placed off-line by an administrative action.
On-line	The network element is working properly.
Failed	The network element is installed and powered on, but is not functioning correctly.
In-test	The Network element is not currently in service due to an administrative action to place it in test.

Example

controller# show ap

AP ID	AP Name	Serial Number	Op State	Availability	Runtime	Connectivity	AP Model	AP Type
1	#1-2F-QA-20	00:12:F2:00:2f:24	Disabled	Offline	3.2-1163.2.5-			
7	None	AP208	Local					
2	#2-2F-Sw-20	00:12:F2:00:30:98	Enabled	Online	3.2-1163.2.5-			
7	L3	AP208	Local					
3	#3-2F-Exec-	00:12:F2:00:17:94	Enabled	Online	3.2-1163.2.5-			
7	L2	AP201	Local					
4	#4-2F-HW-20	00:12:F2:00:2f:3a	Disabled	Offline				
	AP208	Local			None			
5	#5-1F-Front	00:12:F2:00:2e:c4	Disabled	Offline				
	AP208	Local			None			

forti-wifi# show ap 1

AP Table

AP ID	: 1
AP Name	: #1-2F-QA-208
Serial Number	: 00:0c:e6:00:2f:24
Uptime	: 00d:00h:00m:00s
Location	: SunnyvaleSanta Clara
Building	: HQ
Floor	: 2nd floor
Contact	: Sam
Operational State	: Disabled

Availability Status	: Offline
Alarm State	: Critical
Enable High Density	: off
LED Mode	: Normal
AP Init Script	:
Boot Image Version	: 3.09.0003.9.01
FPGA Version	: 8.38.3wmac0:11.0 wmac1:11.0
Runtime Image Version	: 3.2-1163.2.5-71
Connectivity Layer	: None
Dataplane Mode	: tunneled
Link Probing Duration	: 120
AP Model	: AP208
AP Type	: Local

show ap-connectivity

Displays the access point connections.

Syntax `show ap-connectivity`

Command Mode EXEC

Default None

Usage Displays access point connectivity information, including the type of configuration, the discovery protocol used, the connectivity layer, and the IP address.

Examples The following command displays access point connectivity information for all APs:

```
default# show ap-connectivity
```

AP ID	AP Name	IP Configuration	Discovery Protocol	Connectivity	IP Address
1	#1-2F-QA-208	Static	L3-preferred	None	0.0.0.0
16	CustSup	Static	L3-preferred	L3	192.168.9.11
18	Mktg	Static	L3-preferred	L3	192.168.9.14
26	AP-26	DHCP	L2-preferred	L2	0.0.0.0
28	AP-28	Static	L3-preferred	L2	192.168.1.71
29	AP-29	Static	L2-preferred	L2	0.0.0.0

AP Network Connectivity configuration(6)

The following command displays detailed connectivity information for AP 1:

```
default# show ap-connectivity 1
```

AP Network Connectivity configuration

AP ID : 1

```

AP Name           : #1-2F-QA-208
IP Configuration  : Static
Static IP Address  : 192.168.10.21
Static IP Netmask  : 255.255.255.0
Static Default Gateway : 192.168.10.1
Primary DNS Server : 10.0.0.10
Secondary DNS Server : 10.0.0.40
AP Host Name       : Ap4-2F-QA
Discovery Protocol : L3-preferred
Controller Address  : 192.168.10.2
Controller Host Name :
Controller Domain Name :
Connectivity Layer : None
Domain Name         : localdomain
IP Address           : 0.0.0.0
NetMask              : 0.0.0.0
Gateway              : 0.0.0.0
DNS Server 1         : 0.0.0.0
DNS Server 2         : 0.0.0.0
DNS Server 3         : 0.0.0.0
DNS Server 4         : 0.0.0.0
DNS Server 5         : 0.0.0.0
DNS Server 6         : 0.0.0.0
DNS Server 7         : 0.0.0.0
DNS Server 8         : 0.0.0.0

```

Related Commands

- [*show ap on page 627*](#)
- [*show ap-discovered on page 632*](#)
- [*show ap-siblings on page 629*](#)

show ap-discovered

Displays the list of discovered access points and stations.

Syntax

show ap-discovered [*MAC_address*]

MAC_address Optional. Display specific information for this MAC address (station or AP).

Command Mode

EXEC

Default

None

Usage

Displays the access points and stations discovered by the system.

Examples

controller# **show ap-discovered**

ID	MAC Address	Type	Channel	SSID				
BSSID	Last	Previous	Current	Pkts Rx	RF	Band	Name	
16	00:02:2d:66:e1:b0	STATION	6					
00:0c:e6:07:32:c3	00d:00h:00m:20s	0	0	509	unknown	Cust-		
Sup								
16	00:02:b3:d9:1f:54	STATION	6					
00:0f:f7:02:b7:4e	00d:00h:00m:00s	14	13	8768	unknown	Cust-		
Sup								
16	00:02:b3:d9:1f:64	STATION	6					
00:0f:8f:ef:9e:7f	00d:00h:00m:18s	40	40	9	unknown	Cust-		
Sup								
16	00:02:b3:e6:d7:12	STATION	6					
00:40:96:a3:72:22	00d:00h:00m:01s	17	23	1124	unknown	Cust-		
Sup								
16	00:03:2a:00:3c:58	STATION	6					
00:00:00:00:00:00	00d:00h:00m:00s	0	0	3	802.11b	Cust-		
Sup								
16	00:04:f2:00:3a:ae	STATION	6					
00:0c:e6:08:f0:8f	00d:00h:00m:03s	13	13	6	unknown	Cust-		
Sup								

16	00:06:25:09:21:0b STATION	6			
00:0c:e6:06:ad:11 00d:00h:00m:01s	9	10	410	802.11b Cust-Sup	
16	00:0c:85:76:35:ea STATION	6			
00:0c:e6:02:5f:67 00d:00h:00m:00s	20	20	46298	unknown Cust-Sup	
16	00:0c:e6:01:04:ff AP	6	qa-func		
00:0c:e6:01:04:ff 00d:00h:00m:00s	4	4	178772	802.11g Cust-Sup	
16	00:0c:e6:01:29:97 AP	6	forti-default		
00:0c:e6:01:29:97 00d:00h:00m:00s	14	14	774781	802.11b Cust-Sup	
16	00:0c:e6:01:3c:5f AP	6	forti-ess		
00:0c:e6:01:3c:5f 00d:00h:00m:00s	24				

Related
Commands

- [show ap on page 627](#)
- [show ap-connectivity on page 630](#)
- [show ap-siblings on page 629](#)

show ap-redirect

Displays the assignment of APs to controller configuration.

Syntax

```
show ap-redirect ip-subnet <ip_subnet>
show ap-redirect mac-address <mac_addr>
```

ip-subnet <ip_subnet> Shows all or the specified IP subnet address of redirected.

mac-address <mac_addr> Shows all or the specified MAC address to be redirected.

Command Mode

Privileged EXEC

Default

None

Usage

Displays the access points redirection tables.

Examples

The following example show how to view the AP redirect table of MAC addresses:

```
forti-wifi# show ap-redirect mac-address
```

```
AP MAC          Destination Controller
```

```
0:0c:e6:00:01:02 172.10.10.5
```

```
Assignments of APs to controllers(1 entry)
```

Related Commands

[ap-redirect](#) on page 581

show ap-swap

Displays the access point replacement table.

Syntax

show ap-swap

Command Mode

EXEC

Default

None

Usage

Displays access point swap information in the AP Replacement Table. The AP Serial number is the MAC address of AP that is being replaced with the MAC address listed in the New AP Serial Number.

Examples

```
controller# show ap-swap
AP Serial Number      New AP Serial Number
00:0c:e6:00:05:02     00:0c:e6:00:30:98
      AP Replacement Table (1 entry)
controller#
```

Related Commands

[swap ap](#) on page 658

show ess-ap

Displays the ESS-AP table for the access point.

Syntax `show ess-ap ap`

Command Mode AP configuration

Default None

Usage Displays the ESS-AP table information including ESSID, access point name, and BSSID.

Examples controller# `show ess-ap ap 1`

ESS Profile		AP ID	AP Name	IfIndex	Channel	BSSID
forti-ess 16	CustSup	1	6			00:0c:e6:02:5f:67
forti-ess18	Mktg	1	6			00:0c:e6:02:5f:67
forti-ess26	AP-26	1	6			00:0c:e6:01:3c:5f
forti-ess28	AP-28	1	6			00:0c:e6:01:77:df
forti-ess29	AP-29	1	6			00:0c:e6:01:3c:5f
controller#						

show interfaces Dot11Radio

Displays the configuration of AP wireless interfaces.

Syntax

`show interfaces Dot11Radio [ap_id [if_index]]`

ap_id Optional. The ID of the access point.
if_index Optional. The ID of the interface.

Command Mode

EXEC

Default

None

Usage

Displays the configuration of all AP wireless interfaces or optionally, for the specified AP. Enter the ID number to specify a particular access point.

Examples

controller# `show interfaces Dot11Radio`

AP ID	AP Name	IfIndex	Op State	Channel	Short Preamble	AP Mode
16	CustSup	1	Enabled	6	on	Normal
18	Mktg	1	Enabled	6	on	Normal
26	AP-26	1	Enabled	6	on	Normal
28	AP-28	1	Enabled	6	on	Normal
29	AP-29	1	Enabled	6	on	Normal

Wireless Interface Configuration(5 entries)

forti-wifi# `show interfaces Dot11Radio 2`

AP ID	AP Name	IfIndex	AP Model	Admin State	Op State	Channel
Short Preamble	RF Band	AP Mode				

```
2      AP-2      1      AP100      Up      Disabled 6      on
802.11b      Normal
```

Wireless Interface Configuration(1 entry)

```
forti-wifi# show interfaces Dot11Radio 2 1
```

Wireless Interface Configuration

```
AP ID                : 2
AP Name              : AP-2
Interface Index      : 1
AP Model             : AP100
Description          : ieee80211-2-1
Administrative Status : Up
Operational Status   : Disabled
Last Change Time     : 2008/01/16 12:38:28
Radio Type           : RF1
MTU (bytes)          : 2346
Channel              : 6
Short Preamble       : on
RF Band Support      : 802.11b
RF Band Selection    : 802.11b
Antenna Selection    : None
Transmit Power High(dBm) : 21
AP Mode              : Normal
Fixed Channel        : off
Scanning Channels    : 1,2,3,4,5,6,7,8,9,10,11
Protection Mechanism : 802.11-1999
Protection Mode      : auto
Number of Antennas   : 1
Dual abg Support     : off
Fallback Channel     : 0
```

Related Commands

show interfaces Dot11Radio antenna-property

Displays the properties of the AP antennas.

Syntax

```
show interfaces Dot11Radio antenna-property [[ap_ID] ifindex] connector
```

ap_ID	Optional. Displays antenna control information of the specified AP.
ifindex	Optional. Displays antenna control information of the specified AP wireless interface.
connector	Optional. Displays detailed antenna control information of the specified connector.

Command Mode

EXEC

Default

None

Usage

Use this command to display antenna properties. Without arguments, the display shows the properties for all APs. You can specify properties for a specific AP, interface index, or connector location. The properties that are displayed are APID, Interface Index, connector number (left=1, right=2), the RF band, gain, external or internal antenna type, and location.

Examples

controller# **show interfaces Dot11Radio antenna-property**

AP ID	IfIndex	Connector	RF Band	Gain (dBm)	Type	Location
4	1	1	Dual	4	unknown	Left
4	1	2	Dual	0	unknown	Right
4	2	1	Dual	5	unknown	Left
4	2	2	Dual	0	unknown	Right
5	1	1	Dual	4	unknown	Left
5	1	2	Dual	0	unknown	Right
5	2	1	Dual	5	unknown	Left
5	2	2	Dual	0	unknown	Right

6	1	1	Dual	4	External	Left
6	1	2	Dual	4	External	Right
7	1	1	Dual	4	unknown	Left
7	1	2	Dual	0	unknown	Right
7	2	1	Dual	5	unknown	Left
7	2	2	Dual	0	unknown	Right
9	1	1	Dual	5	External	Left
9	1	2	Dual	5	External	Right
1	1	1	Dual	4	External	Left
1	2	1	Dual	5	External	Right
3	1	1	Dual	4	External	Left
10	1	1	Dual	4	External	Left
10	2	1	Dual	5	External	Right
8	1	1	Dual	4	External	Left
2	1	1	Dual	4	External	Left
2	2	1	Dual	5	External	Right

Antenna Property(24)

The following display show the antenna properties for AP 5:

controller# **show interfaces Dot11Radio antenna-property 5**

AP ID	IfIndex	Connector	RF Band	Gain (dBm)	Type	Location
5	2	2	Dual	0	unknown	Right
5	2	1	Dual	5	unknown	Left
5	1	2	Dual	0	unknown	Right
5	1	1	Dual	4	unknown	Left

Antenna Property(4)

The following display show the antenna properties for AP 5, interface 1:

controller# **show interfaces Dot11Radio antenna-property 5 1**

AP ID	IfIndex	Connector	RF Band	Gain (dBm)	Type	Location
5	1	1	Dual	4	unknown	Left
5	1	2	Dual	0	unknown	Right

Antenna Property(2)

The following display show the antenna properties for AP 5, interface 1, connector 1:

```
controller# show interfaces Dot11Radio antenna-property 5 1 1
```

Antenna Property

```
AP ID           : 5
Interface Index  : 1
Connector       : 1
RF Band         : Dual
Antenna Gain (dBi) : 4
Link Type       : Point-To-Multi-Point
Antenna Type    : unknown
Location        : Left
```

Related Commands

[antenna-property](#) on page 576

show interfaces Dot11Radio statistics

Displays the statistics of the radios.

Syntax

show interfaces Dot11Radio statistics *[[ap_ID] ifindex]*

- ap_ID

Optional. Displays statistics for the specified AP.
- ifindex

Optional. Displays statistics for the specified AP wireless interface.

Command Mode

EXEC

Default

None

Usage

Use this command to display statistics for the APs and their interfaces. Without arguments, the display shows the properties for all APs. You can specify properties for a specific AP, and an interface index. The following table describes the statistics:

Statistic	Description
Interface Index	Unique identification number of the wireless interface.
AP ID	Unique numeric identifier for the access point.
AP Name	Name of the access point.
Channel	The operating channel.
Associations	The total number of devices associated to the radio.
Throughput	Total throughput level on the radio.
Channel Utilization	Overall utilization level (in percentage) on the operating channel.
Noise	The noise level in dBm.
Loss Percentage	The overall loss percentage.
Management Percentage	Total percentage of frames dedicated to management traffic.

Statistic	Description
Beacon Percentage	Total percentage of traffic dedicated to beacons.
Probe Percentage	Percentage of probe requests in the air.
Neighborhood	Number of other devices in the area.
Retry Percentage	Percentage of retry frames in the air.

Examples

controller# **show interfaces Dot11Radio statistics**

```
IfIndex AP-ID AP-Name Ch Assoc Thruput Ch-Util Noise Loss% Mgmt% Beacon%
Probe% Neighborhood Retry%
1 102 AP-102-THOMAS-J 6 0 9 40 -64 1 16 6 10 0 2
2 102 AP-102-THOMAS-J 157 1 12 24 -79 99 3 3 0 0 0
1 103 AP-103-Harsh-JA 6 16 2795645 58 -60 13 22 8 14 0 30
2 103 AP-103-Harsh-JA 157 24 58153893 59 -80 0 1 1 0 0 48
1 104 AP-104-POPOV-JA 6 0 48 46 -68 0 18 7 11 0 3
2 104 AP-104-POPOV-JA 157 2 2000 23 -71 3 3 3 0 0 49
1 105 AP-105-KGUHA-JA 6 0 0 38 -73 0 16 6 9 0 0
2 105 AP-105-KGUHA-JA 157 0 0 16 -74 0 4 2 1 0 0
Wireless (802.11) Statistics(8 entries)
```

controller# **show interfaces Dot11Radio statistics 10 1**
Wireless (802.11) Statistics

```
Interface Index : 1
AP ID : 102
AP Name : AP-102-THOMAS-JADE
Channel : 6
Failed Count : 7445442
Retry Count : 0
Multiple Retry Count : 4215324
Frame Duplicate Count : 4836511
RTS Success Count : 152178695
RTS Failure Count : 5244008733372
ACK Failure Count : 68313813
```

WEP Undecryptable Count : 0
FCS Error Count : 54800443737
PLCP Error Count : 6010397952
Transmit Frame Count : 11082548
Multicast Transmit Frame Count : 0
Transmit Fragment Count : 11082548
Multicast Received Frame Count : 994077
Received Fragment Count : 69849074627
Received Retried frame Count : 47635890
Received Unicast frame Count : 707331523
Assigned Station Count : 0
Associated Station Count : 0
Discovered Station Count : 480
Average throughput : 0
Channel Utilization : 40
Qos Discarded Fragment Count : 0
Qos CF Polls Rx Count : 0
Qos CF Polls Unused Count : 0
Qos CF Polls Unusable Count : 0
Qos CF Polls Lost Count : 0
Transmit AMSDU Count : 0
Failed AMSDU Count : 0
Retry AMSDU Count : 0
Multiple Retry AMSDU Count : 0
Transmit Octets In AMSDU Count : 0
AMSDU Ack Failure Count : 0
Received AMSDU Count : 2442
Received Octets In AMSDU Count : 0
Transmit AMPDU Count : 5149202
Transmit MPDUs in AMPDU Count : 9082500
Transmit Octets In AMPDU Count : 4374061387
Received AMPDU Count : 0
MPDUs in Received AMPDU Count : 4303092
Received Octets In AMPDU Count : 0
AMPDU Delimiter CRC Error Count : 0
Implicit BAR Failure Count : 0
Explicit BAR Failure Count : 0

Channel Width Switch Count : 186733328
Frame 20 Mhz Transmit Count : 0
Frame 40 Mhz Transmit Count : 0
Frame 20 Mhz Received Count : 10035323
Frame 40 Mhz Received Count : 0
PSMP Success Count : 0
PSMP Failure Count : 0
Granted RDG Used Count : 0
Granted RDG Unused Count : 0
Transmit Frames in Granted RDG Count : 0
Transmit Octets in Granted RDG Count : 0
Beamforming Count : 0
Dual CTS Success Count : 0
Dual CTS Failure Count : 0
STBCCTS Success Count : 0
STBCCTS Failure Count : 0
Non STBCCTS Success Count : 0
Non STBCCTS Failure Count : 0
RTSLSIG Success Count : 0
RTSLSIG Failure Count : 0
Transmit Retry Limit Exceed Count Unaggr : 0
Transmit Retry Limit Exceed Count Aggr : 0
Transmit Retry Limit Exceed Count Subframe in Aggr : 0
Transmit Retry Limit Exceed Count BAR : 0
Transmit Multiple Retry Count Unaggr : 0
Transmit Multiple Retry Count Subframe in Aggr : 0
Transmit Multiple Retry Count BAR : 0
Number of bytes received : 0
Number of bytes transmitted : 0
Unicast Beacon Loss Threshold Exceeded : 0
Current Noise Level : -76
Loss Percentage : 0
Tx Failed Count by Hardware Retry Exceed : 0
Rx Data for Assigned Stations : 0
Rx Management Frames : 0
Total Rx Management Frames : 0
Total Rx Control Frames : 0

Management Frame Overhead : 17
Transmitted Unicast Frame Count : 0
Received All Data Frame Count : 0
Frames blocked by RF-barrier : 0
Beacon Overhead : 6
Probe Request and Response Overhead : 11
Neighborhood Counter : 0
Potential Beacon Collision Counter : 0
Profile of Beacon Data Rate : H H
Retry Percentage : 0

show regulatory-domain

Displays the regulatory information for the country.

Syntax `show regulatory-domain`

Command Mode Privileged EXEC

Default None

Usage This command displays the regulatory information for the country the controller is configured for.

Examples controller# `show regulatory-domain`
RF Regulatory Domain

```
Country Code           : USA
Country Name           : United States Of America
Default B/G Channel    : 6
Default A Channel      : 40
```

show statistics ap300-diagnostics

Displays the list of AP300 diagnostics statistics per interface.

Syntax `show statistics ap300-diagnostics`

Command Mode Privileged EXEC mode

Default None

Usage

Example This example shows the results of the command `show statistics AP300-diagnostics`.

Master1# `show statistics ap300-diagnostics`

AP-ID	IfIndex	AP-Name	Fatal	HW	INT	Tx	Underrun	INT	Tx	Timeout	INT
Carrier	Sense	Timeout	Rx	Overrun	INT	Rx	EOL	INT			
3	1	3-Guha	0	0		321	0				
48		0									
3	2	3-Guha	0	0		213	0				
306		0									
4	1	4-QA.Facing	0	0		3446	0				
0		0									
4	2	4-QA.Facing	0	0		6689	0				
0		0									
5	1	5-Popov	0	0		687	0				
251		0									
5	2	5-Popov	0	0		322	0				
788		0									
8	1	8-Amazon	0	0		374119	0				
0		0									
8	2	8-Amazon	0	0		14	0				
0		0									
96	1	AP-96	0	0		1775	0				
12		0									

96 0	2	AP-96 1	0	0	0	0
98 0	1	9-GrndConf 0	0	0	3764	0
98 0	2	9-GrndConf 0	0	0	0	0
103 24	1	103-carlos 0	0	0	467	0
103 412	2	103-carlos 1	0	0	356	0
239 0	1	AP-239 0	0	0	7492	0
239 2	2	AP-239 0	0	0	2	0

AP300 Diagnostic Statistics(16 entries)

Master1#

Related
Commands

show statistics station-per-ap

Displays the list of station statistics per AP.

Syntax `show statistics station-per-ap`

Command Mode Privileged EXEC

Default None

Usage This command displays the statistics for each AP's stations.

Examples

```
default# show statistics station-per-ap
AP  AP-Name  If  Station-MAC      Station-IP      SSID      Rx
Rate  Tx Rate  Rx-Pkts      Tx-Pkts      EncrypErr
2   AP-2      1   00:03:7f:bf:08:1e 0.0.0.0         abcjk      0
15              0           229           0
2   AP-2      2   00:40:96:a8:af:f3 172.27.0.70     abcjk      34
52      12881           7330           0
23  AP-23     1   00:16:6f:1a:c8:56 0.0.0.0         diag       0
52      312           765           0

Station Per AP Statistics(3 entries)
```

show statistics top10-ap-problem

Displays a list of the top problem access points.

Syntax `show statistics top10-ap-problem`

Command Mode User EXEC

Default None

Usage Use the `show statistics top10-ap-problem` command to display a list of the top problem access points. Ten access points with the highest number of packet retransmissions, with a minimum of 20% for transmissions. Only downlink packet transmissions are considered because uplink packet losses cannot be reliably computed in a multicell WLAN deployment.

Examples The following command displays the most top problem access points.

```
controller# show statistics top10-ap-problem
```

```
AP  AP Name    If Tx Loss Percentage
```

```
2   #2-2F-Sw- 2   37
```

```
Top 10 problem AP statistics(1 entry)
```

```
controller#
```

[Table 4](#) on page 651 describes the fields of the `show statistics top10-ap-problem` output.

TABLE 4: *Output for show statistics top10-ap-problem*

Field	Description
AP	Unique ID number of the access point.
AP Name	Name of the access point.

TABLE 4: *Output for show statistics top10-ap-problem*

Field	Description
If	Interface number of the AP.
Tx Loss Percentage	Percentage of packets lost during transmission (no acknowledgement).

**Related
Commands**

show statistics top10-ap-talker **on page 653**

show statistics top10-ap-talker

Displays the 10 most active access points, based on the sum of transmission and reception packet rates per minute during the last polling period.

Syntax `show statistics top10-ap-talker`

Command Mode EXEC

Default None

Usage Use the `show statistics top10-ap-talker` command to display the 10 most active access points, based on the sum of transmission and reception packet rates per minute during the last polling period. The top talker access points table shows activity based on the number of frames per minute, not actual bytes transmitted or airtime consumed.

Examples The following command displays the most top active access points.

```
controller# show statistics top10-ap-talker
AP   AP Name   If Rx Frames/min Tx Frames/min

2    #2-2F-Sw- 2  10625300         11452490
3    #3-2F-Exe 1  125023           1360549
6    #6-1F-CS- 1  195022           884976
2    #2-2F-Sw- 1  38201            909269
10   #10-1F-Mk 1  57274            714166
8    #8-1F-Dem 1  113896           325462
10   #10-1F-Mk 2  53540            383962
11   AP-11     2  9329             202435
11   AP-11     1  5860             201866
1    #1-2F-QA- 1  0                0

      Top 10 talker AP statistics(10)
controller#
```

[Table 5](#) on page 654 describes the fields of the `show statistics top10-ap-talker` output.

TABLE 5: *Output for show statistics top10-ap-talker*

Field	Description
AP	Unique ID number of the access point.
AP Name	Name of the access point.
If	Interface number of the AP.
Rx Frames/min	Number of frames received during the last polling period.
Tx Frames/min	Number of frames transmitted during the last polling period.

**Related
Commands**

show statistics top10-ap-problem on page 651

show topoap

Displays the APs seen by the system.

Syntax `show topoap`

Command Mode Privileged EXEC

Default None

Usage Displays access point information including allocated resources, number of neighbors, number attached, and number assigned.

Examples

```
controller# show topoap
```

AP ID	AP Name	RsRq	RsAlloc	Neighbor	Attached
2	#2-2F-Sw-208	0	0	4	2
10	#10-1F-Mktg-208	0	0	5	11
3	#3-2F-Exec-201	0	0	5	7
11	AP-11	0	0	2	0
6	#6-1F-CS-AP201	0	0	4	6
8	#8-1F-DemoArea-	0	0	4	9

AP Wireless Resources(6 entries)

Related Commands [show topoapap](#) on page 656

show topoapap

Displays the AP/AP edge records in the system.

Syntax

show topoapap

Command Mode

Privileged EXEC

Default

None

Usage

This command lists APs that are able to hear one another, similar to the **show ap-siblings** output information. Regardless of what APs display in the output, all APs on the same BSSID are coordinated.

Examples

controller# **show topoapap**
RSSI between APs

Detecting AP ID	Detecting AP Name	Sibling AP ID	Sibling AP Name
26	AP-26	16	CustSup
26	AP-26	18	Mktg
26	AP-26	28	AP-28
26	AP-26	29	AP-29
16	CustSup	26	AP-26
16	CustSup	18	Mktg
16	CustSup	28	AP-28
16	CustSup	29	AP-29
18	Mktg	26	AP-26
18	Mktg	16	CustSup
18	Mktg	28	AP-28
18	Mktg	29	AP-29
28	AP-28	26	AP-26
28	AP-28	16	CustSup
28	AP-28	18	Mktg

28	AP-28	29	AP-29
29	AP-29	26	AP-26
29	AP-29	16	CustSup
29	AP-29	18	Mktg
29	AP-29	28	AP-28
RSSI between APs(20)#			

**Related
Commands**

- [show topoap](#) on page 655
- [show ap-siblings](#) on page 629

swap ap

Configures the MAC address of a replacement AP.

Syntax

```
swap ap <old_mac_address> <new_mac_address>
no swap ap <old_mac_address>
```

- old_mac_address Specifies the MAC address of an AP that is to be replaced
- new_mac_address Specifies the MAC address of the replacement AP

Command Mode

Global Configuration mode

Default

NA

Limitations

An AP can only be replaced with another AP of the same model. (AP300 and AP300i are the same for this purpose.)

Usage

This command updates settings associated an AP ID. Each AP has an ID and a serial number (its MAC address) that are used for tracking purposes. This command equates the serial number of an AP that you want to replace at your site with a serial number of a new AP. By linking the two serial to an AP ID number in a replacement table, the system can update the new AP with the configured features from an old AP. This saves you from having to re-enter settings for the replacement AP. There are three configurations that affect an AP; AP Configuration, Interface Configuration, and ESS Configuration.

The command was originally designed to preserve the configuration of an AP's capability-independent generic settings such as location or building. In release 4.0, the command swap ap also preserves these AP configuration attributes:

Attribute	Preserved in AP Configuration	Preserved in Interface Config	Preserved in ESS Configuration
AP ID	yes	yes	no
AP Name	yes	yes	no

Attribute	Preserved in AP Configuration	Preserved in Interface Config	Preserved in ESS Configuration
Location	yes		no
Building	yes	no	no
Floor	yes	no	no
Contact	yes	no	no
LED Mode	yes	no	no
Connectivity	yes	no	no
Link probing duration	yes	no	no
Channel	no	yes	no
RF Band Selection	no	yes	no
power	no	yes	no
AP mode	no	yes	no
Protection Mechanism	no	yes	no
Protection Mode	no	yes	no
Short preamble	no	yes	no

Use the **no** form of the command to remove an AP entry from the AP replacement table.

Run this command, physically replace the AP, and reboot the system. The replacement table is checked, and then the changes are implemented. Once the new AP is updated, its entry is removed from the replacement table.

Examples

```
controller(config)# swap ap 00:0c:e6:bc:61:4e 00:11:11:11:11:01
controller(config)##show ap-swap
```

```
AP Serial Number      New AP Serial Number
```

```
00:0c:e6:bc:61:4e    00:11:11:11:11:01
```

```
AP Replacement Table(1 entry)
```

Related Commands

show ap-swap on **page 635**

type

Sets the AP antenna connector for the type of antenna.

Syntax

`type {External| External-dual-mode | RS-Antenna}`

Command Mode

Dot11Radio antenna-property configuration

Default

External mode antenna

Usage

This command sets the AP antenna connector port for the type of antenna that is to be used. By default, **External** is used on the antennas shipped with the access points, so no change is needed for APs installed as shipped.

The **External-dual-mode** option must be configured for AP Dual 11a or Dual 11bg operation.

When using the External-dual-mode Antennas:

- For 11bg band, use channels 1 and 11.
- For 11a band, a minimum of 12 channels of separation is recommended (for example channels 44 and 56).
- For proper operation, the radios require 50db to 60db isolation. The isolation will depend on the channel separation, antenna type, antenna gain and physical distance between antennas when mounted. Please contact Fortinet Support for assistance with specific external antenna being considered for use with the AP208 Dual abg feature.
- When choosing the antenna type "External Dual Mode," the default gain is set for 3dBi for 11b/g and 5dBi for 11a. The gain will need to be matched to the characteristics of the selected external antenna and RF band.

The **RS-antenna** parameter is for an optional RS4000 antenna supporting AP200 dual a/b/g mode, using special cables.

When using RS-Antennas:

- For 11b/g band, use channels 1 and 11. Antenna gain is set automatically when antenna type is set to RS-Antenna (that is, default gains for each RF band are pre-set in the system for the RS Antenna, when selected).

- For 11a band, a minimum of 12 channels of separation is recommended (for example, use channels 44 and 56). Antenna gain is set correctly when the RS Antenna is set (that is, default gains for each RF band are pre-set in the system for the RS Antenna, when selected).
- Use with RS-Antenna with patch cables.

Example

This example configures an External-dual-mode antenna:

```
default# configure terminal
default(config)# interface Do11Radio 10 1
default(config-if-802)# antenna-property 1
default(config-if-802-antenna)# type External dual-mode
```

This example configures an RS-Antenna:

```
default# configure terminal
default(config)# interface Do11Radio 10 1
default(config-if-802)# antenna-property 1
default(config-if-802-antenna)# type RS-antenna
```

Related Commands

- [antenna-property](#) on page 576
- [rfband](#) on page 623
- [interface Dot11Radio](#) on page 601

12 Mesh Commands

FortiWLC (SD) 5.2 and later implements mesh support for select AP models when properly licensed. This chapter documents the CLI commands used for supporting the mesh deployment. Note that all actions covered by these commands can also be performed via the WebUI.

For additional details on configuring mesh networks, refer to the *Wireless Backbones with Enterprise Mesh* chapter of the *FortiWLC (SD) Configuration Guide*.



Currently, mesh operation is only supported on the AP1000 series and the AP332e/i models.

- [admin-mode](#) on page 664
- [descr](#) on page 665
- [mesh-ap](#) on page 666
- [mesh-profile](#) on page 667
- [plugnplay](#) on page 668
- [psk](#) on page 669

admin-mode

Allows you to enable or disable the mesh deployment.

Syntax

`admin-mode <enable/disable>`

Enable/Disable

Specify whether the deployment is enabled or disabled.

Command Mode

Mesh configuration

Default

Disabled

Usage

This command is used to activate the current mesh network. When **admin-mode** is enabled, the mesh network is active.

Examples

```
default(15)# configure terminal
default(15)(config)# mesh-profile mp
default(15)(config-mesh)# admin-mode enable
default(15)(config-mesh)# end
```

Related Commands

- [mesh-profile on page 667](#)
- [pluginplay on page 668](#)

descr

Enters a description for the current mesh profile.

Syntax

descr *<description>*

description

A brief (between 0 and 128 characters) description of the selected mesh profile.

Command Mode

Mesh configuration

Default

NA

Usage

This command is used to provide a description for the mesh. The description cannot exceed 128 characters.

Examples

```
default(15)# configure terminal
default(15)(config)# mesh-profile mp
default(15)(config-mesh)# descr "Sample mesh profile."
default(15)(config-mesh)# end
```

Related Commands

- [mesh-profile on page 667](#)
- [psk on page 669](#)

mesh-ap

Adds a specified AP to the current mesh profile.

Syntax

mesh-ap <*number*>

number The AP ID number.

Command Mode

Mesh configuration

Default

NA

Usage

This command is used to add a new AP to the current mesh.

Examples

```
default(15)# configure terminal
default(15)(config)# mesh-profile mp
default(15)(config-mesh)# mesh-ap 2
default(15)(config-mesh)# end
```

Related Commands

- [mesh-profile on page 667](#)
- [descr on page 665](#)
- [psk on page 669](#)

mesh-profile

Enters mesh configuration mode.

Syntax

mesh-profile <*profile*>

profile The name of the mesh profile to be modified.

Command Mode

Global configuration

Default

NA

Usage

This command is used to access mesh properties and make changes by using the other commands documented in this chapter. All mesh-based commands are performed while in mesh configuration mode.

Examples

```
default(15)# configure terminal
default(15)(config)# mesh-profile mp
default(15)(config-mesh)#
```

Related Commands

- [admin-mode](#) on page 664
- [descr](#) on page 665
- [mesh-ap](#) on page 666
- [plugnplay](#) on page 668
- [psk](#) on page 669

plugnplay

Enables or disables the PlugNPlay function on the current mesh.

Syntax

`plugnplay <enable/disable>`

enable/disable Enables or disables PlugNPlay.

Command Mode

Mesh configuration

Default

Disabled

Usage

The PlugNPlay feature allows mesh nodes to be connected wirelessly to an existing mesh, without requiring them to be wired directly to the controller first. When first powered-on, a mesh-capable AP will seek out a mesh deployment within range that has PlugNPlay enabled. If it finds one, it will automatically download the mesh PSK and configuration from the nearest mesh AP.

Note that this AP must still be added to the Mesh AP Table (using the [mesh-ap on page 666](#) command) before it can assume mesh operation.

Examples

```
default(15)# configure terminal
default(15)(config)# mesh-profile mp
default(15)(config-mesh)# plugnplay enable
default(15)(config-mesh)# end
```

Related Commands

- [admin-mode on page 664](#)
- [descr on page 665](#)
- [mesh-profile on page 667](#)

psk

Configures the pre-shared key used for mesh encryption.

Syntax

psk key <*key*>

key The desired encryption key used to protect mesh communications.

Command Mode

Mesh configuration

Default

NA

Usage

This command is used to specify the WPA pre-shared encryption key that is used by mesh nodes to communicate with each other. This key is only used by nodes; end-users do not have to provide it when connecting to the mesh.

Examples

```
default(15)# configure terminal
default(15)(config)# mesh-profile mp
default(15)(config-mesh)# psk key MySharedKey
default(15)(config-mesh)# end
```

Related Commands

- [admin-mode](#) on page 664
- [mesh-profile](#) on page 667
- [pluginplay](#) on page 668

13 Rogue AP Detection Commands

The commands contained in this chapter are used for configuring and displaying information about Rogue AP detection:

- *rogue-ap acl on page 672*
- *rogue-ap aging on page 673*
- *rogue-ap assigned-aps on page 674*
- *rogue-ap blocked on page 675*
- *rogue-ap detection on page 677*
- *rogue-ap mitigation on page 679*
- *rogue-ap mitigation on page 679*
- *rogue-ap mitigation-frames on page 680*
- *rogue-ap operational-time on page 681*
- *rogue-ap scanning-channels on page 682*
- *rogue-ap scanning-time on page 684*
- *show rogue-ap acl on page 685*
- *show rogue-ap blocked on page 686*
- *show rogue-ap globals on page 687*
- *show rogue-ap-list on page 688*

rogue-ap acl

Adds the BSSID of an access point to the permitted access control list (ACL) for the WLAN as an authorized BSSID.

Syntax

```
rogue-ap acl <bssid>  
no rogue-ap acl <bssid>
```

bssid BSSID of the access point to be added to the access control list as a permitted BSSID in the format ff:ff:ff:ff:ff:ff.

Command Mode

Global configuration

Default

None

Usage

Use the **rogue-ap acl** command to specify that an access point with a particular BSSID be added to the ACL as an authorized access point. All ESSs known to the controller are automatically included in the ACL.

A BSSID cannot be listed in the ACL as an authorized BSSID and also listed on the list of blocked BSSIDs. If you want to add a BSSID to the authorized list, and the BSSID is currently on the blocked list, you must remove the BSSID from the blocked list (using the command **no rogue-ap blocked**). Then you can add the BSSID to the authorized list.

Use the **no** form to delete an authorized BSSID entry from the ACL.

Examples

The following command adds the BSSID 00:0e:cd:cb:0f:bc to the ACL as a permitted access BSSID:

```
controller(config)# rogue-ap acl 00:0e:cd:cb:0f:bc  
controller(config)#
```

Related Commands

- [rogue-ap blocked on page 675](#)
- [rogue-ap mitigation on page 679](#)
- [show rogue-ap acl on page 685](#)

rogue-ap aging

Configures the amount of time an undetected rogue AP alarm stays active.

Syntax

rogue-ap aging *<aging-time>*

aging-time Amount of time an alarm for an unknown or blocked BSSID that is no longer detected remains active. Value can be from 60 through 86,400 seconds.

Command Mode

Global configuration

Default

The default rogue AP alarm aging time is 60 seconds.

Usage

This command configures the amount of time an alarm for an unknown or blocked BSSID that is no longer detected remain active. After the aging-time elapses, any rogue AP that is no longer detected is automatically removed from the alarm list and its alarm is cleared.

Examples

The following command sets the rogue AP alarm aging time to 300 seconds:

```
controller(config)# rogue-ap aging 300
controller(config)#
```

Related Commands

[rogue-ap mitigation](#) on page 679

rogue-ap assigned-aps

Configures the number of APs that perform rogue AP mitigation.

Syntax

rogue-ap assigned-aps *<number_aps>*

number_aps Specifies the number of APs that participate in rogue AP mitigation. The valid range is between 1 and 20 APs.

Command Mode

Global configuration

Default

The default number of mitigating APs is 3.

Usage

This command configures the maximum number of APs that will attempt to perform rogue AP mitigation.

In the WLAN, only a subset of APs perform mitigation. This reduces the number of mitigation frames sent over the airwaves while maintaining network throughput performance. The APs that are closest to the rogue AP send mitigation frames.

Examples

The following command sets the number of APs assigned to perform mitigation to 5:

```
controller(config)# rogue-ap assigned-aps 5
controller(config)#
```

Related Commands

[rogue-ap mitigation](#) on page 679

rogue-ap blocked

Specifies the BSSID of an access point to be designated as an unauthorized access point in the WLAN.

Syntax

```
rogue-ap blocked <bssid>  
no rogue-ap blocked <bssid>
```

<i>bssid</i>	BSSID of the access point to be designated as blocked in the ACL, which means the access point is considered unauthorized in the WLAN. Must be specified in hexadecimal format (xx:xx:xx:xx:xx:xx)
--------------	--

Command Mode

Global configuration

Default

None

Usage

Use the **rogue-ap blocked** command to specify that an access point with a particular BSSID be added to the blocked list.

If the rogue AP mitigation mode is “selected” (using the command **rogue-ap mitigation selected**), then only rogue stations connecting to the BSSIDs in this list will be mitigated.

A BSSID cannot be listed in the ACL as an authorized BSSID and also listed on the list of blocked BSSIDs. If you want to add a BSSID to the blocked list, and the BSSID is currently on the authorized list, you must remove the BSSID from the authorized list (using the command **no rogue-ap acl**). Then you can add the BSSID to the blocked list.

If the option for mitigation is to block clients seen on the wire (using the command **rogue-ap mitigation wiredRogue**) and any BSSIDs of clients seen on the wire is added here, only those clients will be blocked on the wire,

Use the **no** form to delete a BSSID entry from the blocked list.

Examples

The following command specifies the BSSID 00:02:2d:61:0a:2c as a blocked BSSID in the ACL:

```
controller(config)# rogue-ap blocked 00:02:2d:61:0a:2c
```

```
controller(config)#
```

Related Commands

- [*rogue-ap acl*](#) **on page 672**
- [*show rogue-ap blocked*](#) **on page 686**

rogue-ap detection

Enables rogue AP detection.

Syntax

```
rogue-ap detection  
no rogue-ap detection
```

Command Mode

Global configuration

Default

Rogue AP detection is disabled by default.

Usage

When you enable rogue AP detection, the scans for and detects access points. Access points that are discovered are compared to an access control list (ACL) that lists access points by their BSSIDs. Access points in the ACL are designated as authorized or blocked. Authorized access points are known access points that are allowed to operate in the WLAN. Blocked access points are considered unauthorized access points in the WLAN.

Use the **no** form to disable rogue AP detection.

Examples

The following command enables rogue AP detection:

```
controller(config)# rogue-ap detection  
controller(config)#
```

Related Commands

- [*rogue-ap acl on page 672*](#)
- [*rogue-ap blocked on page 675*](#)

rogue-ap min-rssi

Sets minimum RSSI threshold level for mitigation.

Syntax

rogue-ap min-rssi <level>

level minimum rogue value (dBm)

Command Mode

Global configuration

Default

RSSI level is -100 by default.

Usage

This command sets the minimum RSSI (Received Signal Strength Indication) level, over which a station will be mitigated. This value (in dBm) determines which AP/stations are rogues. If the RSSI value of an AP/is greater than or equal to the min-rssi level, it is a rogue.

Examples

The following command sets the minimum RSSI level to -80:

```
controller # configure terminal
controller(config)# rogue-ap min-rssi -80
controller(config)#
```

Related Commands

rogue-ap mitigation

Configures the level of rogue AP mitigation.

Syntax

```
rogue-ap mitigation all
rogue-ap mitigation none
rogue-ap mitigation selected
rogue-ap mitigation wiredRogue
```

all	Enables rogue AP mitigation; all BSSIDs detected that are not specified as authorized in the rogue AP ACL are blocked.
none	Disables rogue AP mitigation.
selected	Enables rogue AP mitigation for BSSIDs listed in the blocked list.
wiredRogue	Clients detected on the wired side of the AP will be mitigated.

Command Mode

Global configuration

Default

Rogue AP mitigation is disabled by default.

Usage

Rogue AP mitigation prevents stations from associating with a rogue AP. Enabling rogue AP mitigation allows you to prevent clients using FortiAPs from accessing the network through rogue APs.

Use the **rogue-ap mitigation** command to enable rogue AP mitigation for all BSSIDs not previously listed as authorized, or for BSSIDs listed as blocked BSSIDs, or for rogue clients detected on the wired side of the AP (the corporate network, in many cases).

Examples

This command enables rogue AP mitigation for BSSIDs on the blocked list:

```
controller(config)# rogue-ap mitigation selected
controller(config)#
```

Related Commands

[rogue-ap blocked](#) on page 675

rogue-ap mitigation-frames

Configures the number of rogue AP mitigation frames sent out per channel, per mitigation interval.

Syntax

rogue-ap mitigation-frames *<number_frames>*

number_frames Sets the maximum number of mitigation frames per channel. The valid range is between 1 and 50, with the default set at 10.

Command Mode

Global configuration

Default

10 mitigation frames per channel is configured by default.

Usage

Rogue AP mitigation prevents stations from associating with a rogue AP. This command sets the number of mitigation frames sent in each mitigation interval. This number does not have to match the number of rogue stations on each channel.

Examples

The following command sets the number of mitigation frames per channel to 25:

```
controller(config)# rogue-ap mitigation-frames 25
controller(config)#
```

Related Commands

[rogue-ap detection](#) on page 677

rogue-ap operational-time

Configures amount of time APs spend in operational mode on home channel.

Syntax

rogue-ap operational-time <operational-time>

operational-time Sets the number milliseconds of operational time on the home channel. The valid range is from 100 to 5000 milliseconds. The default setting is 400 milliseconds.

Command Mode

Global configuration

Default

The default setting is 400 milliseconds of operational time.

Usage

If scanning is enabled, this command sets the number of milliseconds spent on operational time (performing normal wireless services) on the home channel. This command is related to the command **rogue-ap scanning-time**. Channels scanned are determined by the command **rogue-ap scanning channels**.

When rogue AP scanning is enabled, the AP spends part of the time scanning channels and part of the time performing normal AP WLAN operations on the home channel. This cycle of scan/operate repeats so quickly that both tasks are performed without noticeable network operation degradation.

Scanning on non-home channels is performed by dedicated scanning APs (set with the **mode** command in the Dot11Radio interface configuration sub-mode) and by APs without associated stations.

Examples

The following command sets the operational time to 2500 milliseconds:

```
controller(config)# rogue-ap operational-time 2500
controller(config)#
```

Related Commands

[rogue-ap mitigation](#) on page 679

rogue-ap scanning-channels

Configures the channels that are scanned in scan mode.

Syntax

rogue-ap scanning-channel <channel-list>

channel-list Lists the set of channels that are to be scanned for rogue APs.
Use a comma separated list from 0 to 256 characters.

Command Mode

Global configuration

Default

The complete set of default channels for the United States are
1,2,3,4,5,6,7,8,9,10,11,36,40,44,48,52,56,60,64,149,153,157,161,165

Usage

If scanning is enabled, this command specifies the set of channels that are scanned for rogue APs.

The channels that are scanned by a particular AP are determined by the model of AP. AP201 models scan all channels on the single interface; AP208 interface 1 scans all channels on the 802.11bg band; interface 2 scans all channels on the 802.11a band.

Scanning is performed by dedicated scanning APs (set with the **mode** command in the Dot11Radio interface configuration sub-mode) and by APs without associated stations.

When rogue AP scanning is enabled, for any given period, the AP spends part of the time scanning channels (determined by the **rogue-ap scanning-time** command), and part of the time performing normal AP WLAN operations on the home channel (determined by the **rogue-ap operational-time** command). This cycle of scan/operate repeats so quickly that both tasks are performed without noticeable network operation degradation.

Examples

The following command sets the scanning channels to 1, 6, 11, 36, 44, 52, 60:

```
controller(config)# rogue-ap scanning-channels 1,6,11,36,44,52,60
controller(config)#
```

Related Commands

- [mode on page 613](#)
- [rogue-ap detection on page 677](#)

- [rogue-ap mitigation](#) **on page 679**
- [rogue-ap operational-time](#) **on page 681**
- [rogue-ap scanning-time](#) **on page 684**

rogue-ap scanning-time

Configures the amount of time APs spends scanning each channel other than the operational channel.

Syntax

rogue-ap scanning-time <*scanning-time*>

scanning-time Sets the number milliseconds of scanning time. The valid range is from 100 to 500 milliseconds. The default setting is 100 milliseconds.

Command Mode

Global configuration

Default

The default setting is 100 milliseconds of scanning time.

Usage

If scanning is enabled, this command sets the number of milliseconds that are spent scanning each channel in the global list of channels. This command is related to the **rogue-ap operational-time** command. The channels that are scanned are determined by the **rogue-ap scanning channels** command.

When rogue AP scanning is enabled, for any given period, the AP spends part of the time scanning channels, and part of the time performing normal AP WLAN operations on the home channel.

Scanning on non-home channels is performed by dedicated scanning APs (set with the **mode** command in the Dot11Radio interface configuration sub-mode) and by APs without associated stations.

Examples

The following command sets the scanning time to 200 milliseconds:

```
controller(config)# rogue-ap scanning-time 200
controller(config)#
```

Related Commands

- [rogue-ap detection](#) on page 677
- [rogue-ap mitigation](#) on page 679
- [rogue-ap operational-time](#) on page 681
- [rogue-ap scanning-channels](#) on page 682

show rogue-ap acl

Displays the rogue AP ACL.

Syntax

show rogue-ap acl

Command Mode

EXEC

Default

None

Usage

Examples

The following command displays the list of access points (specified by BSSID) permitted to operate in the WLAN:

```
controller# show rogue-ap acl
```

BSSID

f4:3c:00:1f:f2:d3

00:0c:e6:cd:cd:cd

00:0c:e6:c2:d5:b1

Allowed APs(3)

Related Commands

[rogue-ap acl](#) on page 672

show rogue-ap blocked

Displays the list of blocked BSSIDs.

Syntax `show rogue-ap blocked`

Command Mode EXEC

Default None

Usage

Examples The following command displays the list of blocked access points (specified by BSSID):

controller# `show rogue-ap blocked`

BSSID	Creation Time	Last Reported Time
00:0c:e6:20:c1:48	2005/08/01 20:35:35	-
Blocked APs(1 entry)		

Related Commands [rogue-ap acl](#) on page 672

show rogue-ap globals

Displays current rogue AP parameter settings.

Syntax `show rogue-ap globals`

Command Mode EXEC

Default None

Usage

Examples The following command displays the current rogue AP parameter settings:

```
controller> show rogue-ap globals
Global Settings
```

```
Detection                               : off
Mitigation                             : none
Rogue AP Aging (seconds)                : 60
Number of Mitigating APs                : 3
Scanning time in ms                     : 100
Operational time in ms                  : 400
Max mitigation frames sent per channel : 10
Scanning Channels                       :
1,2,3,4,5,6,7,8,9,10,11,36,40,44,48,52,
56,60,64,100,104,108,112,116,120,124,128,132,136,140,149,153,157,161,165
RSSI Threshold for Mitigation           : -100
controller>
```

- Related Commands**
- [rogue-ap aging on page 673](#)
 - [rogue-ap detection on page 677](#)
 - [rogue-ap mitigation on page 679](#)

show rogue-ap-list

Displays the list of all rogue APs.

Syntax `show rogue-ap-list`

Command Mode Privileged EXEC

Default None

Usage

Examples The following command displays the list of rogue access points specified by BSSID:

controller# `show rogue-ap-list`

Rogue_AP_MAC	Type	Channel	SSID	BSSID
Fortinet_AP1_ID	Last_AP1		RSSI_AP1	Fortinet_AP2_ID Last_AP2
RSSI_AP2	Fortinet_AP3_ID	Last_AP3		RSSI_AP1 Inactive_audits
00:00:4c:1a:84:9c	STATION	11		
00:0c:e6:96:37:81	4		00d:00h:00m:00s -77	2
00d:00h:00m:00s	-82	0	00d:00h:00m:00s	0
00:03:2a:00:3d:be	STATION	11		
00:0c:e6:96:37:81	2		00d:00h:00m:11s -75	4
00d:00h:00m:11s	-86	0	00d:00h:00m:00s	0
00:03:2a:00:6a:0e	STATION	11		
00:0c:e6:ae:a5:9d	2		00d:00h:00m:02s -74	4
00d:00h:00m:02s	-83	0	00d:00h:00m:00s	0

Related Commands [rogue-ap acl](#) on page 672

14 Quality-of-Service Commands

The commands contained in this chapter are used to configure and display information about the Quality of Service settings:

- [*action*](#) on page 691
- [*avgpacketrates*](#) on page 692
- [*dscp*](#) on page 693
- [*dstip*](#) on page 694
- [*dstip-flow*](#) on page 695
- [*dstip-match*](#) on page 696
- [*dstmask*](#) on page 697
- [*dstport*](#) on page 698
- [*dstport-flow*](#) on page 700
- [*dstport-match*](#) on page 701
- [*firewall-filter-id*](#) on page 702
- [*firewall-filter-id-flow*](#) on page 704
- [*firewall-filter-id-match*](#) on page 706
- [*netprotocol-flow*](#) on page 708
- [*netprotocol-match*](#) on page 709
- [*packet max-length*](#) on page 710
- [*packet min-length*](#) on page 711
- [*packet-min-length-flow*](#) on page 712
- [*packet-min-length-match*](#) on page 713
- [*peakrate*](#) on page 714
- [*priority*](#) on page 715
- [*qoscodec*](#) on page 716
- [*qosrule*](#) on page 719
- [*qosrule-logging-frequency*](#) on page 722
- [*qosrulelogging*](#) on page 723

- [qosvars admission](#) on page 724
- [qosvars bwscaling](#) on page 726
- [qosvars cac-deauth](#) on page 727
- [qosvars calls-per-ap](#) on page 728
- [qosvars calls-per-bssid](#) on page 729
- [qosvars calls-per-interference](#) on page 730
- [qosvars drop-policy](#) on page 731
- [qosvars enable](#) on page 732
- [qosvars intercell-periodicity](#) on page 734
- [qosvars load-balance-overflow](#) on page 735
- [qosvars max-stations-per-radio](#) on page 736
- [qosvars max-stations-per-bssid](#) on page 737
- [qosvars sip-idle-timeout](#) on page 738
- [qosvars station-assign-age](#) on page 739
- [qosvars tcpttl](#) on page 740
- [qosvars ttl](#) on page 741
- [qosvars udpttl](#) on page 742
- [rspecrate](#) on page 743
- [rspecslack](#) on page 744
- [srcip](#) on page 745
- [srcmask](#) on page 746
- [srcport](#) on page 747
- [show phones](#) on page 749
- [show phone-calls](#) on page 750
- [show qoscodec](#) on page 751
- [show qosflows](#) on page 754
- [show qosrule](#) on page 756
- [show qosstats](#) on page 761
- [show qosvars](#) on page 762
- [show statistics call-admission-control](#) on page 764
- [tokenbucketrate](#) on page 766
- [tokenbucketsize](#) on page 768
- [trafficcontrol-enable](#) on page 769

action

Specifies the action a QoS rule performs upon a packet.

Syntax

```
action capture
action drop
action forward
```

capture	Capture the packet and send it up to the designated port. This is the default setting.
drop	Drop the packets matching the rule criteria.
forward	Forward the packets.

Command Mode

Qosrule Configuration

Default

The default action if a QoS rule is matched is to capture packets.

Usage

This command specifies the action to take for packets matching QoS criteria.

- Forward: A flow is given an explicit resource request, bypassing the QoS protocol detector and regardless of whether a QoS protocol was specified.
- Capture: A flow is given an explicit resource request by the QoS protocol detector as specified by the QoS protocol setting. This is the recommended action for static QoS rules that are H323/SIP based.
- Drop: The flow is dropped.

Examples

The following command sets the action performed on packets to dropped:

```
controller(config-qosrule)# action drop
```

Related Commands

- [qosrule on page 719](#)
- [show qosrule on page 756](#)

avgpacketrate

Specifies the average packet rate for the QoS rule.

Syntax

avgpacketrate <*avgpacketrate*>

avgpacketrate The average packet rate is a number from zero to 200 packets per second.

Command Mode

Qosrule configuration

Default

The default setting is zero.

Usage

This command sets the average rate for packets to flow. If the rate is non-zero then the traffic specification (TSpec) token bucket rate must also be non-zero and priority is not allowed to be set to a non-zero value.

Examples

The following command sets the average packet rate flow to 100 packets per second.

```
controller(config-qosrule)# avgpacketrate 100
```

Related Commands

- [priority](#) on page 715
- [qosrule](#) on page 719
- [show qosrule](#) on page 756
- [tokenbucketrate](#) on page 766

dscp

Specifies the DiffServ codepoint class.

Syntax

dscp class

class Specifies the codepoint class. The class must be specified as in RFCs 2474, 2475, and 2597.

Command Mode

Qosrule configuration

Default

cs0 (best effort)

Usage

This command specifies the per-hop forwarding behavior for packets in the flow. It is recommended that you be familiar with RFCs 2475 and 2597 before changing these values.

Examples

The following command disables DSCP:

```
controller(config-qosrule)# dscp disabled
```

Related Commands

- [qosrule on page 719](#)
- [show qosrule on page 756](#)

dstip

Specifies the destination IP address for the QoS rule.

Syntax

dstip <*destination-ip-address*>

destination-ip-address Specifies the destination IP address. The address must be specified as *nnn.nnn.nnn.nnn*.

Command Mode

Qosrule configuration

Default

None

Usage

This command specifies the destination IP address for the QoS rule. The destination IP address, in conjunction with a destination subnet mask, are used as criteria for matching the QoS rule.

Examples

The following command sets the destination IP address:

```
default# configure terminal
default(config)# qosrule 200 netprotocol 6 qosprotocol none
controller(config-qosrule)# dstip 192.14.0.0
```

Related Commands

- [dstmask on page 697](#)
- [dstport-match on page 701](#)
- [qosrule on page 719](#)
- [show qosrule on page 756](#)

dstip-flow

Enables destination IP flow for this qosrule.

Syntax

```
dstip-flow on
dstip-flow off
```

on	Turns on the dstip flow.
off	Turns off the dstip flow.

Command Mode

Qosrule configuration

Default

The default is off.

Usage

This command enables the destination IP flow for the QoS rule.

Examples

The following commands set the destination IP flow on:

```
default# configure terminal
default(config)# qosrule 200 netprotocol 6 qosprotocol none
controller(config-qosrule)# dstip 192.14.0.0
controller(config-qosrule)# dstip-flow on
```

Related Commands

- [dstip-match](#) on page 696
- [show qosrule](#) on page 756

dstip-match

Enables destination IP matching for current qosrule.

Syntax

```
dstip-match on  
dstip-match off
```

on	Turns on the dstip match.
off	Turns off the dstip match.

Command Mode

Qosrule configuration

Default

off

Usage

This command enables the destination IP flow for the QoS rule.

Examples

The following commands set the destination IP match on:

```
default# configure terminal  
default(config)# qosrule 200 netprotocol 6 qosprotocol none  
controller(config-qosrule)# dstip 192.14.0.0  
controller(config-qosrule)# dstip-match on
```

Related Commands

- [show qosrule on page 756](#)
- [dstip-flow on page 695](#)

dstmask

Specifies the destination IP address netmask for the QoS rule.

Syntax

dstmask <*destination-netmask*>

destination-netmask Specifies the subnet mask for the destination IP address. The netmask must be specified as *nnn.nnn.nnn.nnn*.

Command Mode

Qosrule configuration

Default

None.

Usage

This command specifies the subnet mask for the destination IP address for the QoS rule. The destination IP address, in conjunction with a destination subnet mask, are used as criteria for matching the QoS rule.

Examples

The following command sets the destination netmask:

```
controller(config-qosrule)# dstmsk 255.0.0.0
```

Related Commands

- [dstip on page 694](#)
- [dstport-match on page 701](#)
- [qosrule on page 719](#)
- [show qosrule on page 756](#)

dstport

Specifies the destination TCP or UDP port for the QoS rule.

Syntax

dstport <*destination-port*>

destination-port Specifies the destination TCP or UDP port. The port can be from 0 to 65535.

Command Mode

Qosrule configuration

Default

The default port is 0 (specifies any port).

Usage

This command specifies the destination TCP or UDP port used as criteria for matching the QoS rule (zero specifies any port).

The controller watches the traffic passing through it. When it sees packets passing from stations to servers on ports reserved for SIP or H.323 service, it tracks subsequent communication in that sequence and provisions the VoIP call with a level of service appropriate for a VoIP calls.

The port numbers watched are:

- 5060 for SIP service (UDP)
- 1720 for H.323 service (TCP)
- 5200 for Vocera Server

These are the standard port numbers for these services. If your VoIP devices use these ports to communicate with their servers, you do not need to configure VoIP QoS rules on your system.

If your VoIP devices and servers are configured to use different ports, you will need to modify the QoS rules on the controller to match the ports your system uses.

Examples

The following command sets the destination port to 1200:

```
controller(config-qosrule)# dstport 1200
```

Related Commands

- [dstport-match](#) on page 701
- [dstport-flow](#) on page 700
- [dstmask](#) on page 697
- [qosrule](#) on page 719
- [show qosrule](#) on page 756

dstport-flow

Enables destination port flow for a QoS rule.

Syntax

```
dstport-flow on
dstport-flow off
```

on	Turns on the dstport flow.
off	Turns off the dstport flow.

Command Mode

Qosrule configuration

Default

The default port-flow is off.

Usage

This command enables destination port flow for a QoS rule. Use this command if you want to match values that you configured in the protocol number. This only makes a difference if traffic control is on.

Examples

The following command sets the QoS rule 200 destination port to 1200:

```
default# configure terminal
default(config)# qosrule 200 netprotocol 6 qosprotocol none
controller(config-qosrule)# dstport 1200
controller(config-qosrule)# dstport-flow on
```

Related Commands

- [dstport on page 698](#)
- [dstport-match on page 701](#)
- [show qosrule on page 756](#)

dstport-match

Enables destination IP matching for the current QoS rule.

Syntax

`dstport-match on`
`dstport-match off`

<code>on</code>	Turns on the dstport-match.
<code>off</code>	Turns off the dstport-match.

Command Mode

Qosrule configuration

Default

The default port-flow is off.

Usage

This command enables destination port flow for a QoS rule. Use this command if you want to match values that you configured in the protocol number.

Examples

The following command sets the QoS rule 200 destination port to 1200:

```
default# configure terminal
default(config)# qosrule 200 netprotocol 6 qosprotocol none
controller(config-qosrule)# dstport 1200
controller(config-qosrule)# dstport-match on
```

Related Commands

- [dstport on page 698](#)
- [dstport-flow on page 700](#)
- [show qosrule on page 756](#)

firewall-filter-id

Assigns a filter firewall ID, associated by either user or per-ESS, to a QOS rule.

Syntax

firewall-filter-id <filter id>

filter id	Alphanumeric value specifying filter-id associated with this Security Profile. This value defines the firewall policy to be used on the controller when the firewall capability is set to configured .
-----------	---

Command Modes

Security profile configuration and configure qosrule

Default

No default

Usage

This value defines the firewall policy to be used on the controller only when the **firewall capability** is set to **configured**. When firewall capability is configured with a firewall filter ID in a security profile, then the same firewall filter ID should be configured in a Qosrule to take effect.

Examples

The following commands set the firewall filter ID to 10:

```
default(config)# security-profile abc
default(config-security)# firewall-capability configured
default(config-security)# firewall-filter-id 10
default(config-security)# exit
controller# configure terminal
controller(config)# qosrule 3 netprotocol 17 qosprotocol sip
default(config-qosrule)# firewall-filter-id 10
default(config-qosrule)# firewall-filter-id-flow on
default(config-qosrule)# firewall-filter-id-match on
default(config-qosrule)# exit
```

Related Commands

- [firewall-capability on page 425](#)
- [firewall-filter-id on page 702](#)
- [firewall-filter-id-flow on page 704](#)

- [firewall-filter-id-match](#) on page 706
- [security-logging](#) on page 466
- [show security-profile](#) on page 484
- [show qosrule](#) on page 756
- [qosrulelogging](#) on page 723
- [qosrule-logging-frequency](#) on page 722

firewall-filter-id-flow

Assigns a filter firewall ID flow to a QOS rule.

Syntax

```
firewall-filter-id-flow on
firewall-filter-id-flow off
```

on	Turns on the firewall-filter-id-flow.
off	Turns off the firewall-filter-id-flow.

Command Modes

Security profile configuration and configure qosrule

Default

Firewall filter ID flow defaults to off.

Usage

This value defines the firewall policy to be used on the controller only when the **firewall capability** is set to **configured**. When firewall capability is configured with a firewall filter ID in a security profile, then the same firewall filter ID should be configured in a Qosrule to take effect.

Examples

The following commands set the firewall filter ID to 10:

```
default(config)# security-profile abc
default(config-security)# firewall-capability configured
default(config-security)# firewall-filter-id 10
default(config-security)# exit
controller# configure terminal
controller(config)# qosrule 3 netprotocol 17 qosprotocol sip
default(config-qosrule)# firewall-filter-id 10
default(config-qosrule)# firewall-filter-id-match on
default(config-qosrule)# exit
```

Related Commands

- [firewall-capability on page 425](#)
- [firewall-filter-id on page 702](#)

- [firewall-filter-id-flow](#) on page 704
- [firewall-filter-id-match](#) on page 706
- [security-logging](#) on page 466
- [show security-profile](#) on page 484
- [show qosrule](#) on page 756
- [qosrulelogging](#) on page 723
- [qosrule-logging-frequency](#) on page 722

firewall-filter-id-match

Assigns a filter firewall ID flow to a QOS rule.

Syntax

```
firewall-filter-id-match on  
firewall-filter-id-match off
```

on	Turns on the firewall-filter-id-match.
off	Turns off the firewall-filter-id-match.

Command Modes

Security profile configuration and configure qosrule

Default

Firewall filter ID match defaults to off.

Usage

This value defines the firewall policy to be used on the controller only when the **firewall capability** is set to **configured**. When firewall capability is configured with a firewall filter ID in a security profile, then the same firewall filter ID should be configured in a Qosrule to take effect.

Examples

The following commands set the firewall filter ID to 10:

```
default(config)# security-profile abc  
default(config-security)# firewall-capability configured  
default(config-security)# firewall-filter-id 10  
default(config-security)# exit  
controller# configure terminal  
controller(config)# qosrule 3 netprotocol 17 qosprotocol sip  
default(config-qosrule)# firewall-filter-id 10  
default(config-qosrule)# firewall-filter-id-match on  
default(config-qosrule)# exit
```

Related Commands

- [firewall-capability on page 425](#)
- [firewall-filter-id on page 702](#)

- [firewall-filter-id-flow](#) on page 704
- [firewall-filter-id-match](#) on page 706
- [security-logging](#) on page 466
- [show security-profile](#) on page 484
- [show qosrule](#) on page 756
- [qosrulelogging](#) on page 723
- [qosrule-logging-frequency](#) on page 722

netprotocol-flow

Enables netprotocol flow for a QOS rule.

Syntax

```
netprotocol-flow on  
netprotocol-flow off
```

Command Mode

Configure QOS rule mode

Default

Default is off.

Usage

This command enables netprotocol flow for a QOS rule.

Examples

The following commands enable netprotocol flow for QoS rule 3.

```
controller# configure terminal  
controller(config)# qosrule 3 netprotocol 17 qosprotocol sip  
controller(config-qosrule)# netprotocol-flow on  
controller(config-qosrule)# exit
```

Related Commands

- [show qosrule on page 756](#)
- [netprotocol-match on page 709](#)

netprotocol-match

Configures QoS rule netprotocol matching.

Syntax

```
netprotocol-match on  
netprotocol-match off
```

Command Mode

Configure QoS rule mode

Default

Netprotocol match default is off.

Usage

This command enables netprotocol flow for a QoS rule.

Examples

The following commands enable netprotocol flow for QoS rule 3.

```
controller# configure terminal  
controller(config)# qosrule 3 netprotocol 17 qosprotocol sip  
controller(config-qosrule)# netprotocol-match on  
controller(config-qosrule)# exit
```

Related Commands

- [show qosrule on page 756](#)
- [netprotocol-flow on page 708](#)

packet max-length

Configures maximum packet length for a QOS rule.

Syntax

packet Max-length *<number>*

number Number from 0 - 1500

Command Mode

Configure QOSrule mode

Default

Default is 0 (zero)

Usage

This command configures maximum packet length for a QOS rule.

Examples

The following commands set maximum packet length to 80 for QoS rule 3:

```
controller# configure terminal  
controller(config)# qosrule 3 netprotocol 17 qosprotocol sip  
controller(config-qosrule)# packet max-length 80
```

Related Commands

[show qosrule](#) *on page 756*

packet min-length

Configures minimum packet length for a QOS rule.

Syntax

packet min-length <number>

number Number from 0 - 1500

Command Mode

Configure QOSrule mode

Default

Default is 0 (zero)

Usage

This command configures minimum packet length for a QOS rule.

Examples

The following commands set minimum packet length to 80 for QoS rule 3:

```
controller# configure terminal
controller(config)# qosrule 3 netprotocol 17 qosprotocol sip
controller(config-qosrule)# packet-min-length 100
controller(config-qosrule)# packet-min-length-flow on
controller(config-qosrule)# packet-min-length-match on
controller(config-qosrule)# end
```

Related Commands

[show qosrule](#) **on page 756**

packet-min-length-flow

Configures minimum packet length for a QOS rule.

Syntax

packet min-length <number>

number Number from 0 - 1500

Command Mode

Configure QOSrule mode

Default

Default is 0 (zero)

Usage

This command configures minimum packet length for a QOS rule.

Examples

The following commands set minimum packet length to 80 for QoS rule 3:

```
controller# configure terminal
controller(config)# qosrule 3 netprotocol 17 qosprotocol sip
controller(config-qosrule)# packet-min-length 100
controller(config-qosrule)# packet-min-length-flow on
controller(config-qosrule)# end
```

Related Commands

[show qosrule](#) **on page 756**

packet-min-length-match

Enables minimum packet length match for the QOS rule.

Syntax

```
packet-min-length-match on  
packet-min-length-match off
```

Command Mode

Configure QOSrule mode

Default

Packet minimum length matching default is off.

Usage

This command enables minimum packet length for QOS rule matching.

Examples

The following commands enable minimum packet length matching on QoS rule 3:

```
controller# configure terminal  
controller(config)# qosrule 3 netprotocol 17 qosprotocol sip  
controller(config-qosrule)# packet-min-length 100  
controller(config-qosrule)# packet-min-length-match on  
controller(config-qosrule)# end
```

Related Commands

[show qosrule](#) *on page 756*

peakrate

Specifies the traffic specification peak rate for a QoS Codec rule.

Syntax

peakrate *<rate>*

rate Traffic peak rate. The valid value range is 0 to 1,000,000 bytes/second.

Command Mode

QoS Codec configuration

Default

The default traffic peak rate is 0.

Usage

This command specifies the traffic specification (Tspec) peak rate for a QoS Codec rule.

Examples

The following command sets the Tspec peak rate to 1000000:

```
controller(config-qoscodec)# peakrate 1000000
```

Related Commands

[show qoscodec](#) **on page 751**

priority

Specifies the queue priority level for the QoS rule.

Syntax

priority <*priority*>

priority

Specifies the number (0-8) that determines the best effort priority queue. The default is zero. The highest priority is 8.

Command Mode

Qosrule configuration

Default

The default priority level is zero.

Usage

This command specifies a priority level for the QoS rule. QoS is applied with reserved traffic being allocated the first portion of the AP packet transmittal total bandwidth, followed by each priority level (8 to 1), and finally by the best-effort (default) traffic class.

If you enable priority (specify a non-zero value), you cannot specify an average packet rate or token bucket rate.

Examples

The following command sets the priority level to 5:

```
controller(config-qosrule)# priority 5
```

Related Commands

- [avgpacketrate](#) on page 692
- [qosrule](#) on page 719
- [show qosrule](#) on page 756
- [tokenbucketrate](#) on page 766

qoscodec

Specifies a QoS codec entry and enters QoS codec configuration mode.

Syntax

```
qoscodec id codec <codec> qosprotocol <qosproto> tokenbucketrate <token-  
bucketrate> maxdatagramsize <maxdatagramsize> minpolicedunit <minpolice-  
dunit> samplerate <samplerate>
```

```
no qoscodec id
```

<i>id</i>	Unique numeric identifier for the QoS codec rule. The valid value range is 0 through 6,000.
codec <i>codec</i>	<p>The following are valid entries for <i>codec</i>:</p> <p>1016—1016 Audio: Payload Type 1, Bit Rate 16 Kbps</p> <p>default—Contains the default TSpec/ RSpec for unknown codecs or codecs for which there is no entry in the codec translation table</p> <p>dv14—DV14 Audio: Payload Type 5, Bit Rate 32 Kbps</p> <p>dv14.2—DV14.2 Audio: Payload Type 6, Bit Rate 64 Kbps</p> <p>g711a—G711 Audio: Payload Type 8, G.711, A-law, Bit Rate 64 Kbps</p> <p>g711u—G711 Audio: Payload Type 0, G.711, U-law, Bit Rate 64 Kbps</p> <p>g721—G721 Audio: Payload Type 2, Bit Rate 32 Kbps</p> <p>g722—Audio: Payload Type 9, Bit Rate 64 Kbps, 7 KHz</p> <p>g7221—G7221 Audio: Payload Type *, Bit-Rate 24 Kbps, 16 KHz</p> <p>g7221-32—G7221 Audio: Payload Type *, Bit-Rate 32 Kbps, 16 KHz</p> <p>g723.1—G7231 Audio: Payload Type 4, G.723.1, Bit Rate 6.3 Kbps</p> <p>g728—G728 Audio: Payload Type 15, Bit Rate 16 Kbps</p> <p>g729—G729 Audio: Payload Type 16, Bit Rate 8 Kbps</p> <p>g7red—Proprietary MSN Codec Audio: Payload Type *</p> <p>gsm—GSM Audio: Payload Type 3, Bit Rate 13 Kbps</p> <p>h261—H.261 Video</p> <p>h263—H.263 Video</p> <p>lpc—IPC Audio: Payload Type 7, Bit Rate 2.4kbps</p> <p>mpa—MPA Audio: Payload Type 14, Bit Rate 32kbps</p> <p>siren—Proprietary MSN Audio: Payload Type *, Bit Rate 16 Kbps, 16 KHz</p>

qosprotocol <i>qosprotocol</i>	Specifies the QoS protocol: h323 —H.323 (used mainly by Microsoft NetMeeting) none —All other protocols sip —Session Initiation Protocol (SIP)
tokenbucketrate <i>tokenbucketrate</i>	Token bucket rate. The valid value range is 0 to 1,000,000 bytes/second.
maxdatagramsize <i>maxdatagramsize</i>	Maximum packet size. The valid value range is 0 to 1,500 bytes.
minpolicedunit <i>minpolicedunit</i>	Minimum number of policed units. The valid value range is 0 to 1,500 bytes.
samplerate <i>samplerate</i>	Packet rate. The valid value range is 0 to 200 packets/second.

Command Mode

Global configuration

Default

None

Usage

This command creates a QoS Codec entry and enters QoS Codec configuration mode. As shipped, 22 codecs are provided, and each can be edited with this command, using the *id* number as the argument. Use the **no** form to delete an entry from the QoS Codec table. The supplied codecs entries can be viewed with **show qoscodec**, and are:

ID	Codec	Qos Protocol
22	h263	sip
21	h261	sip
20	siren	sip
19	g729	sip
18	g7221-32	sip
17	g7221	sip
16	g711a	sip
15	g723.1	sip
14	gsm	sip
13	g711u	sip
12	default	sip

11	h263	h323
10	h261	h323
9	siren	h323
8	g729	h323
7	g7221-32	h323
6	g7221	h323
5	g711a	h323
4	g723.1	h323
3	gsm	h323
2	g711u	h323
1	default	h323

QoS Codec Rules(22)

Examples

The following command creates a QoS Codec rule 4 that specifies a default codec, no QoS protocol, a token bucket rate of 3333 bytes/ps, a maximum datagram size of 4 bytes, a minimum policed unit of 45 bytes, and a sample rate of 34 packets per second:

```
controller(config)# qoscodec 4 codec default qosprotocol none tokenbucket-
rate 3333 maxdatagramsize 4 minpolicedunit 45 samplerate 34
controller(config-qoscodec)#
```

Related Commands

- [tokenbucketrate](#) on page 766
- [show qoscodec](#) on page 751

qosrule

Creates a QoS rule and enters qosrule configuration mode.

Syntax

```
qosrule <id> netprotocol 6 qosprotocol h323
qosrule <id> netprotocol 6 qosprotocol none
qosrule <id> netprotocol 6 qosprotocol sip
qosrule <id> netprotocol 6 qosprotocol sccp
qosrule <id> netprotocol 6 qosprotocol <other>
qosrule <id> netprotocol 17 qosprotocol h323
qosrule <id> netprotocol 17 qosprotocol none
qosrule <id> netprotocol 17 qosprotocol sip
qosrule <id> netprotocol 17 qosprotocol sccp
qosrule <id> netprotocol 17 qosprotocol <other>
qosrule <id> netprotocol <other> qosprotocol h323
qosrule <id> netprotocol <other> qosprotocol none
qosrule <id> netprotocol <other> qosprotocol sip
qosrule <id> netprotocol <other> qosprotocol sccp
qosrule <id> netprotocol <other> qosprotocol <other>
no qosrule id
```

id

Specifies the ID for the QoS rule. The ID must be a unique number.

netprotocol {6 | 17 | other}

Specifies the flow protocol for the QoS rule. The protocol must be **6** (TCP), **17** (UDP), or *other*. *other* can be any valid protocol number such as 119 for the SRP protocol, used with Spectra-link phones. [Full listing at: <http://www.iana.org/assignments/protocol-numbers>.]

qosprotocol {h323 | none | sip | sccp | other}

Specifies the QoS protocol for the rule. Typically, **none** is appropriate in most environments. If you are also using a QoS protocol detector, you must match the network protocol with the type of QoS protocol. Use the following network protocol and QoS protocol matches:

SIP

H.323

SCCP

other

none

Command Mode

Global configuration

Default

None

Usage

Use this command to create a QoS rule and enter qosrule configuration mode. The controller is preconfigured to detect the bandwidth requirements for a SIP or H.323 call and make a bandwidth reservation. Once you specify the ID and the network and QoS protocol parameters, other parameters such as the port, average packet rate are automatically configured for the rule. Use the **no** form of the command to delete a QoS rule.

If you need to modify other of the QoS rule parameters, use the commands contained in the qosrule mode to fine tune those values.

You normally do not need to configure QoS rules in the controller unless you have special requirements in your configuration. For example:

- You want to drop packets coming from certain ports or IP addresses.
- You want to configure the controller to give priority to traffic other than H.323 or SIP traffic.

You can configure rules to provide priority-based or reserved QoS. QoS is applied with reserved traffic being allocated the first portion of total bandwidth, followed by each priority level, and finally by the best-effort (default) traffic class. For priority-based QoS, you can specify one of eight levels of priority using the **priority** parameter in the rule. You can configure reserved QoS for new applications using the average packet rate and token bucket rate parameters together as the traffic specification (also called TSpec in IETF IntServ RFCs).

Examples

The following command creates rule 3 using the UDP and SIP as the network and QoS protocols, respectively:

```
controller(config)# qosrule 3 netprotocol 17 qosprotocol sip
```

The following command shows the QoS rules that are configured:

```
controller# show qosrule
```

ID	Dst IP	Dst Mask	DPort	Src IP	Src Mask	
SPort	Prot	Firewall	Filter	Qos	Action	Drop
1	0.0.0.0	0.0.0.0	1720	0.0.0.0	0.0.0.0	0
6		h323	capture	head		
2	0.0.0.0	0.0.0.0	0	0.0.0.0	0.0.0.0	
1720	6		h323	capture	head	
3	0.0.0.0	0.0.0.0	5060	0.0.0.0	0.0.0.0	0
17		sip	capture	head		

```
4      0.0.0.0      0.0.0.0      0      0.0.0.0      0.0.0.0
5060  17              sip      capture  head
7      0.0.0.0      0.0.0.0      5200  0.0.0.0      0.0.0.0      0
17              other forward head
8      0.0.0.0      0.0.0.0      0      0.0.0.0      0.0.0.0
5200  17              other forward head

QoS Rules(8)
```

The first two preconfigured QoS rules give priority to H.323 traffic sent to and from TCP port 1720 respectively. The next two QoS rules give priority to SIP traffic sent to and from UDP port 5060 respectively.

**Related
Commands**

- [action](#) on page 691
- [avgpacketrates](#) on page 692
- [dstip](#) on page 694
- [dstmask](#) on page 697
- [dstport-match](#) on page 701
- [priority](#) on page 715
- [srcip](#) on page 745
- [srcmask](#) on page 746
- [srcport](#) on page 747
- [show qosrule](#) on page 756
- [tokenbucketrate](#) on page 766
- [trafficcontrol-enable](#) on page 769

qosrule-logging-frequency

Defines the time interval that logs related to a rule are updated.

Syntax

qosrule-logging-frequency <frequency>

frequency Interval from 30 to 60 seconds, with the default setting at 60.

Command Mode

QoS profile configuration

Default

The frequency is set to 60 seconds.

Usage

The command **qosrule-logging-frequency** defines the time interval that logs related to this rule are updated.

Examples

The following shows the configuration of this parameter in the Per-User Firewall Qos Rules:

```
default# configure terminal
default(config)# qosrule 200 netprotocol 6 qosprotocol none
default(config-qosrule)# dstport 80
default(config-qosrule)# action drop
default(config-qosrule)# firewall-filter-id 1
default(config-qosrule)# qosrule-logging on
default(config-qosrule)# qosrule-logging-frequency 30
default(config-qosrule)# exit
default(config)# exit
default# sh qosrule
```

Related Commands

[*qosrulelogging*](#) on page 723

qosrulelogging

Set QoS rule logging on or off.

Syntax

```
qosrulelogging on  
qosrulelogging off
```

Command Mode

QoS profile configuration

Default

QoS rule logging is off.

Usage

Set QoS rule Syslog logging on or off. When enabled, events that affect qosrules are logged.

Examples

The following command enables logging for QoS rules on the controller default.:

```
default# configure terminal  
default(config)# qosrule 200 netprotocol 6 qosprotocol none  
default(config-qosrule)# qosrulelogging on
```

Related Commands

- [qosrule-logging-frequency](#) on page 722

qosvars admission

Specifies QoS call admission policy.

Syntax

```
qosvars admission admitall
qosvars admission pending
qosvars admission reject
```

admitall	Specifies that all QoS flows are admitted to the QoS traffic class. If the aggregate reserved bandwidth exceeds the available bandwidth, degradation of the entire QoS traffic class results.
pending	Specifies that if no bandwidth is available to reserve, new QoS flows are moved to the best-effort traffic class. When enough bandwidth is released from other QoS flows, the flows that were placed in the best-effort traffic class are upgraded to the QoS traffic class.
reject	Specifies that if no bandwidth is available to reserve, requests for resources are rejected and not the flows themselves. QoS flows are permanently moved to the best-effort traffic class. If additional bandwidth is available at a later time, these QoS flows are not moved to the QoS traffic class.

Command Mode

Global configuration

Default

Admission control is set to **pending** by default.

Usage

Bandwidth reservation is performed based on the SIP call signaling (codecs/ports specified in the SDP body), taking into account the amount of bandwidth available at the APs taking the call and consideration for other active, reserved QoS flows on neighboring APs. This is calculated in time basis, taking into account the actual data rate (1/2/5.5/11 Mbps) of the client in the call, since the number of calls supported vary depending on the data rate and distance of each client.

The selected keyword (**admitall**, **pending**, or **reject**) specifies what happens to a QoS flow (for example, a newly established voice call) that requests air resources that are not available at that time.

Examples

The following command changes the admission control policy to reject requests for resources, if bandwidth is not available:


```
controller(config)# qosvars admission reject
```

Related Commands

[show qosvars](#) *on page 762*

qosvars bwscaling

Specifies bandwidth scaling for QoS flows.

Syntax

qosvars bwscaling <value>

value

Specify a value from 1 to 100 to indicate percentage of scaling.

Command Mode

Global configuration

Default

The default bandwidth scaling is set to 100%.

Usage

This command specifies how bandwidth is scaled. A value under 100% reduces the amount of resources that can be reserved, allowing resources for best-effort traffic in a fully loaded environment.

Examples

The following command configures bandwidth scaling to 40%.

```
controller(config)# qosvars bwscaling 40
```

Related Commands

[show qosvars](#) on page 762

qosvars cac-deauth

Configures optional 802.11 de-authentication.

Syntax

```
qosvars cac-deauth on
qosvars cac-deauth off
```

Command Mode

Global configuration

Default

The default setting for this command is **off**.

Usage

This command controls the behaviour of the system when the originator of a call exceeds the available CAC (Call Admission Control) resources. When set to **on**, the system sends an 802.11 De-authentication frame to push the client to an alternate BSS. When set to **off** (default setting), the system sends a modified INVITE message to the SIP Server. When CAC is enabled, as the set call level threshold is neared for the AP or BSSID, the admin can configure actions to occur when the limit is reached, which can include one of the following actions:

- For generic SIP servers, send a 486_BusyHere message to reject the call.
- For some cases where needed, send a modified INVITE message to SIP server.
- Other cases where needed, send a modified INVITE or a 486_BusyHere message to reject the call, which contains the X-CallAdmission SIP extension header.

Examples

The following command enables the CAC De-authentication feature:

```
controller(config)# qosvars cac-deauth on
```

Related Commands

[show qosvars](#) on page 762

qosvars calls-per-ap

Configures maximum number of calls per AP.

Syntax

qosvars calls-per-ap *<max_calls>*

max_calls Specifies the maximum number of simultaneous calls for APs. Valid values are from 0 to 256. By default, 0 is set, which allows no calls.

Command Mode

Global configuration

Default

The default setting for this command is 0.

Usage

This command sets a threshold for the maximum number of calls per AP. This command implements the Call Admission Control (CAC) feature, which ensures a consistent level of voice quality by setting a threshold for the number of calls per AP. As an AP nears the set threshold, CAC denies new SIP connections until enough bandwidth is available to effectively handle the resulting media stream

When the call limit for the AP is exceeded, all new calls receive a 486_BusyHere response until the number of calls is less than the specified threshold. On handoff from one AP to another, if there are no resources available in the second AP, the call is classified as Pending/Best-effort until the needed resources are available.

Examples

The following command sets the maximum number of calls per AP to 12:

```
controller(config)# qosvars calls-per-ap 12
```

Related Commands

- [qosvars cac-deauth on page 727](#)
- [qosvars calls-per-bssid on page 729](#)
- [show qosvars on page 762](#)
- [show statistics call-admission-control on page 764](#)

qosvars calls-per-bssid

Configures maximum number of calls per BSSID.

Syntax

qosvars calls-per-bssid *<max_calls>*

max_calls	Specifies the maximum number of simultaneous calls for BSSIDs. The allowable range of calls is from 0 to 1023. By default, 0 is set, which allows all calls.
-----------	--

Command Mode

Global configuration

Default

The default setting for this command is 0.

Usage

This command, with an argument other than the default (0), sets a threshold for the maximum number of calls per BSS. This command implements the Call Admission Control (CAC) feature, which ensures a consistent level of voice quality by setting a threshold for the number of calls per BSS. As a BSS nears the set threshold, CAC denies new SIP connections until enough bandwidth is available to effectively handle the resulting media stream

When the call limit for the BSS is exceeded, all new calls receive a 486_BusyHere response until the number of calls is under the specified threshold. By default, *max_calls* is set to 0, meaning there is no limit for that BSSID and the per-AP limit applies. For CAC, both the **qosvars calls-per-ap** and the **qosvars calls-per-bssid** are validated.

Examples

The following command sets the maximum number of calls to 14:

```
controller(config)# qosvars calls-per-bssid 14
```

Related Commands

- [qosvars cac-deauth](#) on page 727
- [qosvars calls-per-ap](#) on page 728
- [show qosvars](#) on page 762
- [show statistics call-admission-control](#) on page 764

qosvars calls-per-interference

Configures maximum number of calls per interference region.

Syntax

qosvars calls-per-interference <max_calls>

max_calls	Specifies the maximum number of simultaneous calls per interference region. Valid values are from 0 to 256. By default, it is set to 0.
-----------	---

Command Mode

Global configuration

Default

The default setting for this command is 0.

Usage

This command sets the maximum number of calls in an interference region, regardless of the number of access points sharing that region. A given geographical region has a fixed wireless capacity. If there is one access point located at that region, that access point utilizes the entire wireless capacity. If more than one AP is present in that region, the APs must share the fixed wireless capacity. This feature sets a limit for the number of calls in a given region, and based on the number of APs sharing the region, the fixed number of calls will be distributed among the APs.

Examples

The following command sets the maximum number of calls per interference region to 75:

```
controller(config)# qosvars calls-per-interference 75
```

Related Commands

- [qosvars cac-deauth on page 727](#)
- [qosvars calls-per-bssid on page 729](#)
- [show qosvars on page 762](#)
- [show statistics call-admission-control on page 764](#)

qosvars drop-policy

Specifies the QoS global drop policy.

Syntax

```
qosvars drop-policy head  
qosvars drop-policy tail
```

head	Specifies that if new packets arrive after the queue has reached its maximum length, they are allowed in the queue, and old information in the queue is replaced with the new information. Select this option for applications that use constant-rate real-time flows, such as voice applications, where minimizing delay is generally more important than reducing packet loss.
tail	Specifies that if new packets arrive after the queue has reached its maximum length, they are dropped. Select this option if you are using applications with built-in flow control.

Command Mode

Global configuration

Default

The drop policy is set to **tail**.

Usage

This command specifies whether packets are dropped from the head or the tail of the QoS packet queue if packets overflow the queue.

Examples

The following command sets the drop policy to **head**:

```
controller(config)# qosvars drop-policy head
```

Related Commands

[show qosvars](#) on page 762

qosvars enable

Enables QoS.

Syntax

```
qosvars enable
qosvars no enable
```

Command Mode

Global configuration

Default

QoS is enabled by default.

Usage

This command enables QoS settings globally.

Examples

The following command enables QoS settings globally:

```
default(config)# qosvars enable
default(config)#
```

The following command disables QoS:

```
controller(config)# qosvars no enable
controller(config)#
```

Related Commands

- [qosvars admission on page 724](#)
- [qosvars bwscaling on page 726](#)
- [qosvars cac-deauth on page 727](#)
- [qosvars calls-per-ap on page 728](#)
- [qosvars calls-per-bssid on page 729](#)
- [qosvars drop-policy on page 731](#)
- [qosvars load-balance-overflow on page 735](#)
- [qosvars max-stations-per-radio on page 736](#)
- [qosvars max-stations-per-bssid on page 737](#)
- [qosvars tcpttl on page 740](#)
- [qosvars ttl on page 741](#)

- [qosvars udpttl](#) on page 742
- [show qosvars](#) on page 762

qosvars intercell-periodicity

This command is not supported in this release.

Syntax

`qosvars intercell-periodicity`

Command Mode

Global configuration

Default

Usage

Although this command is listed in the CLI, it should not be used and is not supported.

qosvars load-balance-overflow

Enables or disables client load balancing across APs and BSSIDs.

Syntax

```
qosvars load-balance-overflow on
qosvars load-balance-overflow off
```

Command Mode

Global configuration

Default

The default setting for this command is off (disabled).

Usage

This command is used to enable or disable client load balancing across BSSIDs and APs, ensuring a level of QoS for client call sessions. This command is used in conjunction with the commands **qosvars max-stations-per-radio** and **qosvars max-stations-per-bssid**. When the maximum number of stations is reached, new call associations are distributed among APs and BSSIDs in a round-robin fashion, evening out the distribution if this command is set to **on**.

Examples

The following command enables client load balancing overflow protection:

```
controller(config)# qosvars load-balance-overflow on
```

Related Commands

- [qosvars max-stations-per-radio on page 736](#)
- [qosvars max-stations-per-bssid on page 737](#)
- [show qosvars on page 762](#)

qosvars max-stations-per-radio

Configures client load balancing across radios.

Syntax

qosvars max-stations-per-radio <max_stations>

max_stations	Specifies the maximum number of clients (stations) that can associate with a radio. By default, this is set to 128 and can range from 0 to 384.
--------------	---

Command Mode

Global configuration

Default

The default setting for this command is 128.

Usage

This command is used to configure client load balancing across AP radios, ensuring a level of QoS for client call sessions. This command sets the maximum number of stations that can be assigned to a single radio. When the maximum number of stations is reached, new call associations can be distributed among radios and BSSIDs in a round-robin fashion, evening out the distribution if the **qosvars load-balance overflow** command is set to **on**.

Examples

The following command sets the maximum number of stations per radio to 15:

```
controller(config)# qosvars max-stations-per-radio 15
```

Related Commands

- [qosvars load-balance-overflow](#) on page 735
- [qosvars max-stations-per-bssid](#) on page 737
- [show qosvars](#) on page 762

qosvars max-stations-per-bssid

Configures client load balancing across BSSIDs.

Syntax

qosvars max-stations-per-bssid <max_stations>

max_stations	Specifies the maximum number of clients (stations) that can associate with a BSSID. By default, this is set to 0. A maximum of 1023 stations can be set.
--------------	--

Command Mode

Global configuration

Default

The default setting for this command is 0, which basically disables client load balancing.

Usage

This command is used to configure client load balancing across BSSIDs, ensuring a level of QoS for client call sessions. This command sets the maximum number of stations that can be assigned to an BSSID. When the maximum number of stations per BSSID is reached, new call associations can be distributed among BSSIDs in a round-robin fashion, evening out the distribution if the **qosvars load-balance overflow** command is set to on.

If you want to perform client load balancing across VirtualCells, then it is recommended that you set the value of **max-stations-per-bssid** to be the number of devices in the network divided by the number of VirtualCells (or BSSIDs). If you expect that at some times there may be additional devices beyond that joining the network, you should also set **qosvars load-balance overflow** to **on** so that once the maximum number of stations limit is reached, round-robin will be performed to balance new client assignments.

Examples

The following command sets the maximum number of stations per BSSID to 30:

```
controller(config)# qosvars max-stations-per-bssid 30
```

Related Commands

- [qosvars max-stations-per-radio](#) on page 736
- [qosvars load-balance-overflow](#) on page 735
- [show qosvars](#) on page 762

qosvars sip-idle-timeout

Configures SIP call timeout interval.

Syntax

qosvars sip-idle-timeout <*seconds*>

seconds

Specifies the maximum amount of time in seconds a call can idle. The *interval* can be from 5 to 3600, with 150 seconds being the default.

Command Mode

Global configuration

Default

The default setting for this command is 150 seconds.

Usage

This command is used to configure the amount of time a call can idle before it must be answered (the setting is a part of CAC). The valid range is from 5 to 3600 seconds, with the default setting at 120 seconds.

Examples

The following command sets the maximum idle interval to 1000 seconds:

```
controller(config)# qosvars sip-idle-timeout 1000
```

Related Commands

[show qosvars](#) on page 762

qosvars station-assign-age

Configures number of seconds allowed for station association.

Syntax

qosvars stations-assign-age <*seconds*>

seconds	Specifies the maximum amount of time in seconds a station is allowed to associate. The <i>interval</i> can be from 5 to 2000, with 30 seconds being the default.
---------	--

Command Mode

Global configuration

Default

The default setting for this command is 30 seconds.

Usage

This command is used to configure the amount of time an AP caches a client's state while waiting for a Probe or Authenticate request/response sequence with a BSS to complete. The default 30 seconds is adequate for most sites and should not be changed unless recommended by Fortinet **Customer Support** Technical Assistance Center.

Examples

The following command sets the maximum association interval to 10 seconds:

```
controller(config)# qosvars stations-assign-age 10
```

Related Commands

[show qosvars](#) on page 762

qosvars tcpttl

Specifies the TCP QoS time to live (TTL) value.

Syntax

qosvars tcpttl <value>

value The value can be between 0 to 65,535 seconds.

Command Mode

Global configuration

Default

The default TCP TTL is zero seconds.

Usage

This command specifies the amount of time in seconds the QoS TCP flow can be inactive before the flow is moved to the best-effort class.

Examples

The following command sets the QoS TCP flow TTL to 65535:

```
controller(config)# qosvars tcpttl 65535
```

Related Commands

[show qosvars](#) **on page 762**

qosvars ttl

Specifies the default QoS time to live (TTL) value.

Syntax

qosvars ttl <value>

value The value can be between 0 to 65,535 seconds.

Command Mode

Global configuration

Default

The default time-to-live value is 0.

Usage

This command specifies the amount of time that the system recognizes and holds resources for an ongoing flow (for example, a voice call) without seeing any packet activity.

As an example, if the default time-to-live value is set to 300 seconds, a call can continue for 5 minutes without any packets being exchanged before the resources for it are relinquished. Applications that use silence suppression might require higher time-to-live values.

Examples

The following command sets the default QoS TTL value to 300 seconds (5 minutes):

```
controller(config)# qosvars ttl 300
```

Related Commands

[show qosvars](#) **on page 762**

qosvars udpttl

Specifies the UDP QoS time to live (TTL) value.

Syntax

qosvars udpttl <value>

value The value can be between 0 to 65,535 seconds.

Command Mode

Global configuration

Default

The default setting for this command is 0.

Usage

This command specifies the amount of time in seconds the QoS UDP flow can be inactive before the flow is moved to the best-effort class.

Examples

The following command sets the QoS UDP flow TTL to 65535:

```
controller(config)# qosvars udpttl 65535
```

Related Commands

[show qosvars](#) **on page 762**

rspecrate

Specifies the reservation spec rate for a QoS Codec rule.

Syntax

rspecrate <*rate*>

rate Specifies the reservation spec rate. From 0 to 1,000,000 bytes/second.

Command Mode

QoS Codec configuration

Default

The default reservation spec rate is 0 bytes/second.

Usage

This command specifies the reservation spec (Rspec) rate for a QoS Codec rule.

Examples

The following command sets the Rspec rate to 1,000,000 bytes/second:

```
controller(config-qoscodec)# rspecrate 1000000
```

Related Commands

[show qoscodec](#) **on page 751**

rspecslack

Specifies the reservation spec slack for a QoS Codec rule.

Syntax

rspecslack <*slack*>

slack Specifies the reservation spec slack. From 0 to 1,000,000 bytes/second.

Command Mode

QoS Codec configuration

Default

The default reservation spec slack is 0 bytes/second.

Usage

This command specifies the reservation spec (Rspec) slack for a QoS Codec rule.

Examples

The following command sets the Rspec slack to 1000000:

```
controller(config-qoscodec)# rspecslack 1000000
```

Related Commands

[show qoscodec](#) **on page 751**

srcip

Specifies the source IP address for the QoS rule.

Syntax

srcip <source-ip-address>

source-ip-address Specifies the source IP address. The address must be specified as *nnn.nnn.nnn.nnn*.

Command Mode

Qosrule configuration

Default

None

Usage

This command specifies the source IP address for the QoS rule. The source IP address, in conjunction with a source subnet mask, are used as criteria for matching the QoS rule.

Examples

The following command sets the source IP address:

```
controller(config-qosrule)# srcip 192.20.0.0
```

Related Commands

- [show qosrule on page 756](#)
- [srcmask on page 746](#)
- [srcport on page 747](#)
- [qosrule on page 719](#)

srcmask

Specifies the source IP address netmask for the QoS rule.

Syntax

srcmask <*source-netmask*>

source-netmask

Specifies the subnet mask for the source IP address. The netmask must be specified as *nnn.nnn.nnn.nnn*.

Command Mode

Qosrule configuration

Default

NA

Usage

This command specifies the subnet mask for the source IP address for the QoS rule. The source IP address, in conjunction with a source subnet mask, are used as criteria for matching the QoS rule.

Examples

The following command sets the source netmask:

```
controller(config-qosrule)# srcmsk 255.0.0.0
```

Related Commands

- [srcip on page 745](#)
- [srcport on page 747](#)
- [qosrule on page 719](#)
- [show qosrule on page 756](#)

srcport

Specifies the source TCP or UDP port for the QoS rule.

Syntax

srcport <source-port>

source-port Specifies the source TCP or UDP port. The port can be from 0 to 65535.

Command Mode

Qosrule configuration

Default

The default port is 0 (specifies any port).

Usage

This command specifies the source TCP or UDP port used as criteria for matching the QoS rule (zero specifies any port).

The controller watches the traffic passing through it. When it sees packets passing from stations to servers on ports reserved for SIP or H.323 service, it tracks subsequent communication in that sequence and provisions the VoIP call with a level of service appropriate for a VoIP calls.

The port numbers watched are:

- 5060 for SIP service (UDP)
- 1720 for H.323 service (TCP)

These are the standard port numbers for these services. If your VoIP devices use these ports to communicate with their servers, you do not need to configure VoIP QoS rules on your system.

If your VoIP devices and servers are configured to use different ports, you will need to modify the QoS rules on the controller to match the ports your system uses.

Examples

The following command sets the source port to 1200:

```
controller(config-qosrule)# srcport 1200
```

Related Commands

- [srcip](#) on page 745
- [srcmask](#) on page 746
- [qosrule](#) on page 719
- [show qosrule](#) on page 756

show phones

Shows all registered phones.

Syntax `show phones`

Command Mode Privileged EXEC

Default None

Usage This command shows all phones on the system that have been registered. Information includes the MAC address and IP address of the client phone, the name of the AP it is associated with, the type of phone, the username associated with the phone, and the SIP server handling the call..

Examples The following command shows all phones that have registered with the system:

controller# **show phones**

MAC Server	IP	AP ID	AP Name	Type	Username
00:0f:86:12:1d:7c 10.6.6.103	10.0.220.119	1	AP-1	sip	5381
Phone Table(1 entry)					

controller#

Related Commands [show phone-calls](#) on page 750

show phone-calls

Shows all active calls.

Syntax `show phone-calls`

Command Mode Privileged EXEC

Default NA

Usage This command shows all active calls on the system.

Examples The following command shows all active calls on the system:

controller# `show phone-calls`

From MAC	From IP	From AP	From AP Name	From Username
From Flow Pending	To MAC	To IP	To AP	To AP Name
To Username	To Flow	Pending	Type	State
00:0f:86:12:1d:7c	10.0.220.119	1	AP-1	5381
100 off	00:00:00:00:00:00	10.0.220.241	0	
69	101 off	sip	connected	

Phone Call Table(1 entry)

Related Commands [show phones](#) on page 749

show qoscodec

Displays a summary of the QoS Codec rules.

Syntax

`show qoscodec <id>`

id Optional. Specifies the number of the QoS Codec rule.

Command Mode

Privileged EXEC

Default

The default for this command is to show all configured QoS Codec rules.

Usage

This command displays all QoS Codec rules, or displays a specific QoS Codec rule with the optional argument.

The detailed codec rule provides the following information:

ID	Unique numeric identifier for the QoS Codec rule.
Codec	Specifies the Codec type.
Token Bucket Rate	Specifies the token bucket rate.
Token Bucket Size	Specifies the size of the token bucket.
Peak Rate	Specifies the traffic specification peak rate.
Maximum Packet Size	Specifies the maximum packet size.
Minimum Policed Unit	Specifies the minimum policed unit size.
Reservation Rate	Specifies the reservation rate.
Reservation Slack	Specifies the reservation slack.
Packet Rate	Specifies the flow packet rate.
QoS Protocol	Specifies the QoS protocol: <ul style="list-style-type: none">• SIP• H.323

Examples

The following command displays all configured QoS Codec rules:

```
controller> show qoscodec
```

ID	Codec	Qos Protocol
----	-------	--------------

22	h263	sip
21	h261	sip
20	siren	sip
19	g729	sip
18	g7221-32	sip
17	g7221	sip
16	g711a	sip
15	g723.1	sip
14	gsm	sip
13	g711u	sip
12	default	sip
11	h263	h323
10	h261	h323
9	siren	h323
8	g729	h323
7	g7221-32	h323
6	g7221	h323
5	g711a	h323
4	g723.1	h323
3	gsm	h323
2	g711u	h323
1	default	h323

QoS Codec Rules(22)

The following command displays QoS Codec rule 4:

```
controller> show qoscodec 4
```

QoS Codec Rules

ID	: 4
Codec	: g723.1
Token Bucket Rate (0-1,000,000 bytes/second)	: 2100
Token Bucket Size (0-16,000 bytes)	: 128
Peak Rate (0-1,000,000 bytes/second)	: 2500

Maximum Packet Size (0-1,500 bytes) : 64
Minimum Policed Unit (0-1,500 bytes) : 0
Reservation Rate (0-1,000,000 bytes/second) : 2100
Reservation Slack (0-1,000,000 microseconds) : 10000
Packet Rate (0-200 packets/second) : 33
QoS Protocol : h323

**Related
Commands**

- [*peakrate*](#) on page 714
- [*qoscodec*](#) on page 716
- [*rspecrate*](#) on page 743
- [*rspecslack*](#) on page 744
- [*tokenbucketsize*](#) on page 768

show qosflows

Displays all QoS flows.

Syntax `show qosflows`

Command Mode Privileged EXEC

Default None

Usage Use the `show qosflows` command to display all active and pending QoS flows.

Examples The following command displays QoS flows:

```
controller# show qosflows
ID      Source IP      Source Destination IP  Dest  Prot  Token Average Sta-
tus
                                     Port      Port      BRate BRate
12      10.6.6.103        0      192.168.10.172    5060  17
16      10.6.6.103        0      192.168.10.161    5060  17
19      10.6.6.103        0      192.168.10.177    5060  17
24      10.6.6.103        0      192.168.10.157    5060  17
25      10.6.6.103        0      192.168.10.180    5060  17
26      10.6.6.103        0      192.168.10.150    5060  17
28      10.6.6.103        0      192.168.10.178    5060  17
13      10.6.6.103        0      192.168.10.143    5060  17
controller#
```

[Table 6](#) on page 755 describes fields in show qosflows output.

TABLE 6: *Output for show qosflows*

Field	Description
ID	Unique numeric identifier for the QoS flow.
Source IP	Source IP address, in conjunction with a destination subnet mask, used as criteria for matching the QoS rule.
Source Port	Source TCP or UDP port used as criteria for matching the QoS rule (zero specifies any port).
Destination IP	Destination IP address, in conjunction with a destination subnet mask, used as criteria for matching the QoS rule.
Destination Port	Destination TCP or UDP port used as criteria for matching the QoS rule (zero specifies any port).
Prot	Network protocol: Specifies whether the flow is TCP (6) or UDP (17) or other.
Token BRate	Token bucket rate (bytes/second).
Average BRate	Average bucket rate (bytes/second).
Status	Reservation status.

show qosrule

Displays the QoS rules that are configured for the system.

Syntax

```
show qosrule
show qosrule <rule>
```

rule Specifies the ID of a QoS rule.

Command Mode

Privileged EXEC

Default

Shows all QoS rules that are configured.

Usage

This command displays all QoS rules, or displays a specific QoS rule with the optional argument. When a rule is specified with the command, the additional information about the priority of the rule and traffic control setting is included.

The display provides the following information:

ID	Unique numeric identifier for the QoS rule.
Dst IP (Destination IP)	This IP address, in conjunction with a destination subnet mask, are used as criteria for matching the QoS rule.
Dst Mask (Destination Netmask)	The subnet mask for the destination IP address.
DPort (Destination Port)	The destination TCP or UDP port used as criteria for matching the QoS rule (zero specifies any port).
Src IP (Source I)P	The source IP address, in conjunction with the source subnet mask, are used as criteria for matching the QoS rule.
Src Mask (Source Net-mask)	Subnet mask of the source IP address.
SPort (Source Port)	Source TCP or UDP port used as criteria for matching the QoS rule (zero specifies any port).

Prot (Network Protocol)	Shows whether the flow is TCP (6) or UDP (17) or other. If you are using a QoS protocol detector, the network protocol matches the type of QoS protocol: UDP: SIP TCP: H.323 TCP: SCCP
Firewall Filter	The ID assigned to this Firewall Filter qosrule.
Qos (QoS Protocol)	The QoS protocol can be: SIP H.323 SCCP Other
Average Packet Rate	Averaged flow packet rate.
Action	Specifies what the rule does with packets: Forward: A flow is given an explicit resource request, bypassing the QoS protocol detector and regardless of whether a QoS protocol was specified. Capture: The system, using a QoS protocol detector, analyzes the flow for its resource requirements. Drop: The flow is dropped.
Drop (Drop Policy)	Identifies what happens to packets that arrive when the queue is full: Head: New packets that arrive after the queue has reached its maximum length are allowed in the queue, and old information in the queue is replaced with the new information. Tail: New packets that arrive after the queue has reached its maximum length are dropped.
Token Bucket Rate	Specifies the Token Bucket Rate (bytes/second).
Priority	Specifies the priority level assigned to the queue.
Traffic Control	Specifies whether traffic control is being enforced. Traffic control can be: On Off
DiffServe Codepoint	Identifies the DiffServ setting in use, or DiffServ Disabled if no setting is in use.

Examples

The following command displays all QoS rules:

```
controller> show qosrule
```

ID	Dst IP	Dst Mask	DPort	Src IP	Src Mask	
SPort	Prot	Firewall	Filter	Qos	Action	Drop
1	0.0.0.0	0.0.0.0	1720	0.0.0.0	0.0.0.0	0
6		h323	capture	head		
2	0.0.0.0	0.0.0.0	0	0.0.0.0	0.0.0.0	
1720	6	h323	capture	head		
3	0.0.0.0	0.0.0.0	5060	0.0.0.0	0.0.0.0	0
17		sip	capture	head		
4	0.0.0.0	0.0.0.0	0	0.0.0.0	0.0.0.0	
5060	17	sip	capture	head		
7	0.0.0.0	0.0.0.0	5200	0.0.0.0	0.0.0.0	0
17		other	forward	head		
8	0.0.0.0	0.0.0.0	0	0.0.0.0	0.0.0.0	
5200	17	other	forward	head		
2001	10.0.0.10	255.255.255.255	53	192.168.37.0	255.255.255.0	
0	17 ab10	none	forward	head		
2002	10.0.0.40	255.255.255.255	53	192.168.37.0	255.255.255.0	
0	17 ab10	none	forward	head		
2003	192.168.37.4	255.255.255.255	0	192.168.37.0	255.255.255.0	
0	0 ab10	none	forward	head		
4001	10.0.0.0	255.0.0.0	0	192.168.37.0	255.255.255.0	
0	0 ab10	other	drop	head		
4002	192.168.0.0	255.255.224.0	0	192.168.37.0	255.255.255.0	
0	0 ab10	none	drop	head		
4003	192.168.64.0	255.255.192.0	0	192.168.37.0	255.255.255.0	
0	0 ab10	none	drop	head		
4004	192.168.128.0	255.255.128.0	0	192.168.37.0	255.255.255.0	
0	0 ab10	none	drop	head		
4005	192.168.48.0	255.255.240.0	0	192.168.37.0	255.255.255.0	
0	0 ab10	none	drop	head		
4006	192.168.40.0	255.255.248.0	0	192.168.37.0	255.255.255.0	
0	0 ab10	none	drop	head		
4007	192.168.32.0	255.255.252.0	0	192.168.37.0	255.255.255.0	
0	0 ab10	none	drop	head		
4008	192.168.38.0	255.255.254.0	0	192.168.37.0	255.255.255.0	
0	0 ab10	none	drop	head		

4009	192.168.36.0	255.255.255.0	0	192.168.37.0	255.255.255.0
0	0	ab10	none drop	head	
4010	192.168.37.0	255.255.255.0	0	192.168.37.0	255.255.255.0
0	0	ab10	none drop	head	
4011	172.16.0.0	255.255.0.0	0	192.168.37.0	255.255.255.0
0	0	ab10	none drop	head	
4012	172.17.0.0	255.255.0.0	0	192.168.37.0	255.255.255.0
0	0	ab10	none drop	head	
4013	172.18.0.0	255.255.0.0	0	192.168.37.0	255.255.255.0
0	0	ab10	none drop	head	
4014	172.26.0.0	255.255.0.0	0	192.168.37.0	255.255.255.0
0	0	ab10	none drop	head	
4015	172.27.0.0	255.255.0.0	0	192.168.37.0	255.255.255.0
0	0	ab10	none drop	head	
4016	0.0.0.0	0.0.0.0	0	192.168.37.0	255.255.255.0
0	0	ab10	none forward	head	

QoS and Firewall Rules(25 entries)

The following command displays QoS rule 1:

```
controller> show qosrule 1
```

QoS and Firewall Rules

ID	: 1
Id Class flow class	: none
Destination IP	: 0.0.0.0
Destination IP match	: none
Destination IP flow class	: none
Destination Netmask	: 0.0.0.0
Destination Port	: 1720
Destination Port match	: on
Destination Port flow class	: none
Source IP	: 0.0.0.0
Source IP match	: none
Source IP flow class	: none
Source Netmask	: 0.0.0.0
Source Port	: 0
Source Port match	: none
Source Port flow class	: none

```

Network Protocol          : 6
Network Protocol match    : on
Network Protocol flow class : none
Firewall Filter ID        :
Filter Id match           : none
Filter Id Flow Class      : none
Packet minimum length     : 0
Packet Length match       : none
Packet Length flow class  : none
Packet maximum length     : 0
QoS Protocol              : h323
Average Packet Rate       : 0
Action                    : capture
Drop Policy               : head
Token Bucket Rate         : 0
Priority                   : 0
Traffic Control           : off
DiffServ Codepoint        : cs0
Qos Rule Logging          : off
Qos Rule Logging Frequency : 60

```

Related Commands

- [*avgpacketrates*](#) on page 692
- [*dstip*](#) on page 694
- [*dstmask*](#) on page 697
- [*dstport-match*](#) on page 701
- [*priority*](#) on page 715
- [*qosrule*](#) on page 719
- [*srcip*](#) on page 745
- [*srcmask*](#) on page 746
- [*srcport*](#) on page 747
- [*tokenbucketrate*](#) on page 766
- [*trafficcontrol-enable*](#) on page 769

show qosstats

Displays QoS statistics.

Syntax `show qosstats`

Command Mode Privileged EXEC

Default None

Usage Displays the following QoS global statistics:

- H.323, SIP and total session counts
- H.323, SIP and total rejected counts
- H.323, SIP and total pending counts
- QoS active flow count
- Qos pending flow count

Examples

```
controller> show qosstats
Global Quality-of-Service Statistics
Session Count                : 0
H.323 Session Count          : 0
SIP Session Count            : 0
Rejected Session Count       : 0
Rejected H.323 Session Count : 0
Rejected SIP Session Count   : 0
Pending Session Count        : 0
Pending H.323 Session Count  : 0
Pending SIP Session Count    : 0
Active Flows                  : 0
Pending Flows                 : 0
```

The Active Flows and Pending Flows include the H.323/SIP flows as well as any flow configured in the QoS rules.

show qosvars

Displays QoS global parameters.

Syntax

show qosvars

Command Mode

Privileged EXEC

Default

None

Usage

This command shows the QoS global parameter settings. Use the **qosvars** commands in the Related Commands section to configure settings for these parameters.

Examples

The following command shows the default settings for the QoS parameters:

```
controller> show qosvars
```

Global Quality-of-Service Parameters

```
On/Off                      : on
Admission Control           : admitall
Drop Policy                  : head
Default Time-to-live (seconds) : 0
UDP Time-to-live (seconds)   : 0
TCP Time-to-live (seconds)   : 0
Bandwidth Scaling (percent)  : 100
Intercell Periodicity (ms)   : 30
Maximum Calls Per AP         : 0
Maximum Calls Per Interference Region : 0
Maximum Stations Per AP      : 128
Maximum Stations Per BSSID    : 0
Load Balance Overflow        : off
Maximum Calls Per BSSID      : 0
CAC Deauth                   : off
Station Assignment Age Time   : 30
```

SIP Idle Timeout (seconds) : 120

Related Commands

- [*qosvars admission*](#) **on page 724**
- [*qosvars bwscaling*](#) **on page 726**
- [*qosvars cac-deauth*](#) **on page 727**
- [*qosvars calls-per-ap*](#) **on page 728**
- [*qosvars calls-per-bssid*](#) **on page 729**
- [*qosvars drop-policy*](#) **on page 731**
- [*qosvars enable*](#) **on page 732**
- [*qosvars load-balance-overflow*](#) **on page 735**
- [*qosvars max-stations-per-radio*](#) **on page 736**
- [*qosvars max-stations-per-bssid*](#) **on page 737**
- [*qosvars tcpttl*](#) **on page 740**
- [*qosvars ttl*](#) **on page 741**
- [*qosvars udpttl*](#) **on page 742**

show statistics call-admission-control

Displays Call Admission Control (CAC) statistics.

Syntax

```
show statistics call-admission-control ap
show statistics call-admission-control bss
```

Command Mode

Privileged EXEC

Default

None

Usage

This command shows the CAC statistics per AP or BSS. For either the AP or BSS, it shows the current number of active calls as well as the cumulative number of calls that have been rejected as a result of reaching the Maximum Number of Calls setting. The cumulative number of rejected calls per BSS and AP are reset when either the controller or AP reboots, respectively. Use the **qosvars** commands listed under Related Commands below to configure settings for these parameters.

Examples

The following command shows the CAC statistics for APs:

```
controller> show statistics call-admission-control ap
```

```
AP ID Current Calls Cumulative Rejected Calls
```

```
1      0              0
```

```
Call Admission Control AP Statistics(1 entry)
```

The following command shows the CAC statistics for BSS:

```
controller> show statistics call-admission-control bss
```

```
BSSID              Current Calls Cumulative Rejected Calls
```

```
00:12:f2:30:97:49 0              0
```

```
00:12:f2:4e:9b:ce 0              0
```

```
00:12:f2:de:ec:6f 0              0
```


Call Admission Control BSS Statistics(3 entries)

Related Commands

- [qosvars calls-per-ap](#) **on page 728**
- [qosvars calls-per-bssid](#) **on page 729**

tokenbucketrate

Specifies the token bucket rate for the QoS rule.

Syntax

tokenbucketrate <*tokenbucketrate*>

tokenbucketrate Specifies the token bucket rate. The rate can be from 0 to 1,000,000 bytes per second. The default is 0.

Command Mode

Qosrule configuration

Default

The default token bucket rate is 0.

Usage

This command specifies the rate at which tokens are placed into an imaginary token bucket. Each flow has its own bucket, to which tokens are added at a fixed rate. To send a packet, the system must remove the number of tokens equal to the size of the packet from the bucket. If there are not enough tokens, the system waits until enough tokens are in the bucket.

If priority is enabled, you cannot specify a token bucket rate.

The relationship of token bucket rate to maximum bandwidth is as follows:

<u>TokenBucketRate</u>	<u>Max Bandwidth</u>
1000	8Kbps
5000	40Kbps
12500	125Kbps
125000	1Mbps
625000	5Mbps
1000000	8Mbps (Maximum Value)

$\text{tokenbucketrate} = x/8$, where x is the preferred maximum bandwidth

Examples

The following commands set the token bucket rate to 3333, then reset it to 1,000,000:

```
controller # configure terminal
controller(config)# qoscodec 4 codec default qosprotocol none tokenbucket-
rate 3333 maxdatagramsize 4 minpolicedunit 45 samplerate 34
controller(config-qosrule)# tokenbucketrate 1000000
```

Related Commands

- [priority](#) on page 715
- [qosrule](#) on page 719
- [show qosrule](#) on page 756
- [tokenbucketsize](#) on page 768

tokenbucketsize

Specifies the token bucket size.

Syntax

tokenbucketsize <size>

size Specifies the token bucket size from 0 to 16,000 bytes.

Command Mode

QoS Codec configuration

Default

The default token bucket size is 8 Kbytes. Usage

This command specifies the size of the token bucket.

Examples

The following command sets the token bucket size to 10,000 bytes:

```
controller(config-qoscodec)# configure terminal
controller(config)# qoscodec 4 codec default qosprotocol none tokenbucket-
rate 3333 maxdatagramsize 4 minpolicedunit 45 samplerate 34
controller(config-qoscodec)# tokenbucketsize 10000
```

Related Commands

- [qoscodec](#) on page 716
- [tokenbucketrate](#) on page 766
- [show qoscodec](#) on page 751

trafficcontrol-enable

Enables traffic control policy for the QoS rule. The **no trafficcontrol** command disables traffic control policy.

Syntax

```
trafficcontrol-enable  
no trafficcontrol
```

Command Mode

Qosrule configuration

Default

The default is traffic control disabled.

Usage

Use this command to enable traffic control. Enabling traffic control restricts the flow (explicit, detected, and best-effort) to the rate you specified with the [avgpacketrate on page 692](#) command. Packets above that rate are dropped.

Examples

The following first enables traffic control, followed by the command to disable traffic control:

```
controller(config-qosrule)# trafficcontrol-enable  
controller(config-qosrule)# no trafficcontrol
```

Related Commands

- [avgpacketrate on page 692](#)
- [qosrule on page 719](#)
- [show qosrule on page 756](#)

15 SNMP Commands

The commands contained in this chapter configure and show the system SNMP settings. SNMPv3 architecture incorporates new descriptions for SNMP entities (Managers, Agents, Proxy Forwarders), updated message formats, and Standard MIBs used to configure access to entities. New SNMPv3 features include: user authentication using entity shared secret keys along with message time stamps, data secrecy using encryption, and control of user access to MIB information based on the need to know.

- [*reload-snmp*](#) on page 772
- [*show snmp-community*](#) on page 773
- [*show snmp-trap*](#) on page 774
- [*show snmpv3-user*](#) on page 775
- [*snmp-filter-config*](#) on page 776
- [*snmpv3-user*](#) on page 777
- [*snmpv3-user auth-key*](#) on page 778
- [*snmpv3-user auth-protocol*](#) on page 779
- [*snmpv3-user priv-key*](#) on page 780
- [*snmpv3-user priv-protocol*](#) on page 781
- [*snmpv3-user target ip-address*](#) on page 782
- [*snmp start and snmp stop*](#) on page 783
- [*snmp-server community*](#) on page 784
- [*snmp-server contact*](#) on page 785
- [*snmp-server description*](#) on page 786
- [*snmp-server location*](#) on page 787
- [*snmp-server trap*](#) on page 788
- [*show snmp-filter-config*](#) on page 789

reload-snmp

Restarts the SNMP process.

Syntax

`reload-snmp`

Command Mode

Privileged EXEC

Default

None

Usage

Use this command to reload the SNMP process. The command can be used, for example, when SNMP does not respond to incoming SNMP packets.

Examples

default# `reload-snmp`

show snmp-community

Displays the IP address and privileges in this community.

Syntax `show snmp-community`

Command Mode Privileged EXEC

Default None

Usage Use this command to display information about the SNMP community, including IP address and read/write privileges.

Examples `default# show snmp-community`

SNMP Community	Client IP	Privilege
public	0.0.0.0	read-only

SNMP Community Management(1 entry)

Related Commands [snmp-server community](#) on page 784

show snmp-trap

Shows the SNMP trap community.

Syntax `show snmp-trap`

Command Mode Privileged EXEC

Default None

Usage Use this command to view the IP address(es) in the trap community.

Examples

```
controller# show snmp-trap
SNMP Trap Management
Trap Community          Destination IP
32                      10.10.1.1
      SNMP Trap Management(1 entry)
controller#
```

Related Commands [snmp-server trap](#) on page 788

show snmpv3-user

Displays SNMPv3 user information.

Syntax `show snmpv3 user`

Command Mode EXEC mode

Default none

Usage Use this command to see the following information:

```
snmpv3# sh snmpv3-user
User Name          AuthProt  PrivProt  Target IP      Auth Key      Priv
Key
NoAuthNoPriv       no-auth  no-priv   192.168.221.101
MD5AuthNoPriv      md5-auth no-priv   192.168.203.150 123456789
SHAAuthNoPriv      sha-auth no-priv   192.168.46.235  456789123
MD5AuthDESPriv     md5-auth des-priv  192.168.10.251  123456789
456123987
SHAAuthDESPriv     sha-auth des-priv  192.168.98.220  456789741
741852963
SNMPv3 User Configuration(5)
```

- Related Commands**
- [snmpv3-user on page 777](#)
 - [snmpv3-user auth-key on page 778](#)
 - [snmpv3-user auth-protocol on page 779](#)
 - [snmpv3-user priv-key on page 780](#)
 - [snmpv3-user priv-protocol on page 781](#)
 - [snmpv3-user target ip-address on page 782](#)
 - [snmpv3-user target ip-address on page 782](#)
 - [show snmpv3-user on page 775](#)

snmp-filter-config

Configure SNMP interface filter based on the table:

- Ap-Assigned table
- AP-Discovered table
- AP-Neighbor table
- AP-Neighbor detail table

Syntax

snmp-filter-config <parameters>

The parameters are:

- ap-assigned
- ap-discovered
- ap-neighbor
- ap-neighbor-detail

Command Mode

Global Configuration

Default

none

Usage

Use this command to filter the SNMP interface:

```
MC3200(15)# configure terminal
MC3200(15)(config)# snmp-filter-config ap-discovered
MC3200(15)(config)#
```

Related Commands

[show snmp-filter-config](#) on page 789

snmpv3-user

Creates new or opens an existing SNMPv3 user name to configure.

Syntax

`snmpv3-user <name>`

Command Mode

Configuration mode

Default

none

Usage

This command starts the process of configuring an SNMPv3 user. Use the listed Related Commands to further define the user.

Example

This example creates the SNMPv3 user MWP.

```
Master1 # configure terminal
Master1(config)# snmpv3-user ?
<Name>                Enter the SNMPv3 User name.
Master1(config)# snmpv3-user MWP
Master1(config-snmpv3-user)#
```

Related Commands

- [snmpv3-user auth-key on page 778](#)
- [snmpv3-user auth-protocol on page 779](#)
- [snmpv3-user priv-key on page 780](#)
- [snmpv3-user priv-protocol on page 781](#)
- [show snmpv3-user on page 775](#)
- [snmpv3-user target ip-address on page 782](#)

snmpv3-user auth-key

Configures an SNMPv3 secret key.

Syntax

auth-key <authentication key>

Command Mode

Configuration mode

Default

none

Usage

Before you can use this command, you have to create an SNMPv3 user or open an existing user configuration as shown in the example.

Example

This example opens the SNMPv3 user MWP, then assigns the authentication key 8h8h8h.

```
Master1 # configure terminal
Master1(config)# snmpv3-user ?
<Name>                Enter the SNMPv3 User name.
Master1(config)# snmpv3-user MWP
Master1(config-snmpv3-user)# auth-key 8h8h8h
```

Related Commands

- [snmpv3-user](#) on page 777
- [snmpv3-user auth-protocol](#) on page 779
- [snmpv3-user priv-key](#) on page 780
- [snmpv3-user priv-protocol](#) on page 781
- [show snmpv3-user](#) on page 775
- [snmpv3-user target ip-address](#) on page 782

snmpv3-user auth-protocol

Configures authentication protocol for SNMPv3 USM users.

Syntax

```
snmpv3-user auth-protocol md5-auth
snmpv3-user auth-protocol no-auth
snmpv3-user auth-protocol sha-auth
```

md5-auth	HMAC MD5 authentication protocol for SNMPv3 USM user
no-auth	No authentication protocol for SNMPv3 USM user
sha-auth	HMAC SHA Authentication protocol for SNMPv3 USM user

Command Mode

Privileged EXEC mode

Default

none

Usage

Before you can use this command, you have to create an SNMPv3 user or open an existing user configuration as shown in the example.

Example

This example opens the SNMPv3 user MWP, then assigns the authentication protocol sha-auth.

```
Master1 # configure terminal
Master1(config)# snmpv3-user ?
<Name>                Enter the SNMPv3 User name.
Master1(config)# snmpv3-user MWP
Master1(config-snmpv3-user)# auth-protocol sha-auth
```

Related Commands

- [snmpv3-user on page 777](#)
- [snmpv3-user auth-protocol on page 779](#)
- [snmpv3-user priv-key on page 780](#)
- [snmpv3-user priv-protocol on page 781](#)
- [show snmpv3-user on page 775](#)
- [snmpv3-user target ip-address on page 782](#)

snmpv3-user priv-key

Configures SNMPv3 secret key.

Syntax

snmpv3-user <name>

Command Mode

Configuration mode

Usage

Before you can use this command, you have to create an SNMPv3 user or open an existing user configuration as shown in the example.

Example

This example opens the SNMPv3 user MWP, then assigns the privacy key 8h8h8h.

```
Master1 # configure terminal
Master1(config)# snmpv3-user ?
<Name>                Enter the SNMPv3 User name.
Master1(config)# snmpv3-user MWP
Master1(config-snmpv3-user)# priv-key 8h8h8h
```

Related Commands

- [snmpv3-user on page 777](#)
- [snmpv3-user auth-protocol on page 779](#)
- [snmpv3-user priv-key on page 780](#)
- [snmpv3-user priv-protocol on page 781](#)
- [show snmpv3-user on page 775](#)
- [snmpv3-user target ip-address on page 782](#)

snmpv3-user priv-protocol

Configures privacy protocol for SNMPv3 USM users.

Syntax

```
priv-protocol des-priv  
priv-protocol no-priv
```

des-priv	DES Privacy protocol for SNMPv3 USM user
no-priv	No privacy protocol for SNMPv3 USM user

Command Mode

Configuration mode

Default

none

Usage

Before you can use this command, you have to create an SNMPv3 user or open an existing user configuration as shown in the example.

Example

This example opens the SNMPv3 user MWP, then assigns the privacy protocol des-priv.

```
Master1 # configure terminal  
Master1(config)# snmpv3-user ?  
<Name> Enter the SNMPv3 User name.  
Master1(config)# snmpv3-user MWP  
Master1(config-snmpv3-user)# priv-protocol des-priv
```

Related Commands

- [snmpv3-user on page 777](#)
- [snmpv3-user auth-protocol on page 779](#)
- [snmpv3-user priv-key on page 780](#)
- [snmpv3-user priv-protocol on page 781](#)
- [show snmpv3-user on page 775](#)
- [snmpv3-user target ip-address on page 782](#)

snmpv3-user target ip-address

Configures the IP address for the snmpv-3 user.

Syntax

snmpv3-user target ip-address <XXX.XXX.XXX.XXX>

Command Mode

Configuration mode

Default

none

Usage

Before you can use this command, you have to create an SNMPv3 user or open an existing user configuration as shown in the example.

Example

This example opens the SNMPv3 user MWP, then assigns the IP address 172.23.34.9.

```
Master1 # configure terminal
Master1(config)# snmpv3-user ?
<Name>                Enter the SNMPv3 User name.
Master1(config)# snmpv3-user MWP
Master1(config-snmpv3-user)# target ip-address 172.23.34.9
```

Related Commands

- [snmpv3-user on page 777](#)
- [snmpv3-user auth-protocol on page 779](#)
- [snmpv3-user priv-key on page 780](#)
- [snmpv3-user priv-protocol on page 781](#)
- [show snmpv3-user on page 775](#)
- [snmpv3-user target ip-address on page 782](#)

snmp start and snmp stop

Starts and stops SNMP. Displays SNMP status.

Syntax

```
snmp start  
snmp stop  
snmp status
```

Command Mode

Privileged EXEC

Default

None

Usage

Use this command to start and stop the SNMP process. Once SNMP is started, SNMP event messages are generated, and interaction with 3rd party SNMP-based programs is possible.

Examples

The following command starts SNMP:

```
controller# snmp start
```

Related Commands

snmp-server community

Configures an SNMP community.

Syntax

```
snmp-server community <community-string> <client_IP_address> ro
snmp-server community <community-string> <client_IP_address> rw
no snmp-server community <client_IP_address>
no snmp-server community 0.0.0.0
no snmp-server community <community-string>
no snmp-server community public <client_IP_address>
no snmp-server community public 0.0.0.0
no snmp-server community public <community-string>
```

<i>community-string</i>	Text string up to 32 alphanumeric characters long. Do not use spaces or special characters.
<i>client-ip-address</i>	IP address associated with the SNMP read/write community. To specify a wildcard and allow all servers access, use 0.0.0.0.
ro rw	Type ro to allow read-only access to the MIB, or type rw to allow read-write access to the MIB

Command Mode

Global configuration

Default

NA

Usage

The SNMP community acts as a password to authenticate messages sent between the SNMP server and SNMP client. The SNMP community string is transmitted in clear text. Use the **no** form of the command to delete a community entry by client IP address or all servers (0.0.0.0).

Examples

The following command configures a read-only community, using the string **commstring1** as password, and allowing only the server with an IP address of **10.3.4.5**:

```
controller(config)# snmp-server community commstring1 10.3.4.5 ro
```

Related Commands

[show snmp-community](#) on page 773

snmp-server contact

Configures the contact person for the controller.

Syntax

snmp-server contact <*contact*>

contact Contact person from 1 to 255 characters.

Command Mode

Global configuration

Default

None

Usage

Use this command to identify the contact person for the controller.

Examples

```
controller(config)# snmp-server contact Joe
controller(config)#
```

Related Commands

- [snmp-server description on page 786](#)
- [snmp-server location on page 787](#)

snmp-server description

Description of the controller.

Syntax

snmp-server description <*descr*>

descr Description of the SNMP server from 1 to 255 characters.

Command Mode

Global configuration

Default

NA

Usage

Use this command to give the controller a description.

Examples

```
controller(config)# snmp-server description corp_manager
controller(config)#
```

Related Commands

- [snmp-server location](#) on page 787
- [snmp-server contact](#) on page 785

snmp-server location

Configures a description location for the controller.

Syntax

snmp-server location <location>

location

Text string from 1 to 255 characters that describes the location of the controller.

Command Mode

Global configuration

Default

None

Usage

Use this command to describe the controller's location.

Examples

```
controller(config)# snmp-server location san_jose_california
controller(config)#
```

Related Commands

- [snmp-server contact](#) on page 785
- [snmp-server description](#) on page 786

snmp-server trap

Configures an SNMP trap community.

Syntax

snmp-server trap <community-string> <client-ip-address>

<i>community-string</i>	Name of the SNMP community. The name can be up to 32 alphanumeric characters long. Do not include spaces or special characters in the name. The SNMP community acts as a password to authenticate messages sent between the SNMP server and SNMP client.
<i>client-ip-address</i>	IP address of the SNMP trap receiver that is listening for SNMP traps generated by the controller. To disable this feature, and allow all servers, use 0.0.0.0.

Command Mode

Global configuration

Default

None

Usage

Use the **snmp-server trap** command to create an SNMP trap community. You specify the SNMP trap receiver (using the *client-IP-address*) that listens for SNMP traps generated by the controller and the SNMP community. The SNMP community is transmitted in clear text.

Use the **no** form of the command to delete a snmp server trap community entry.

Examples

The following command configures an SNMP trap community using **commstring1** as the community string and specifying **10.3.4.5** as the trap receiver:

```
controller(config)# snmp-server trap commstring1 10.3.4.5
controller(config)#
```

Related Commands

[show snmp-community](#) on page 773

show snmp-filter-config

Displays the SNMP filtering configuration parameters.

Syntax

show snmp-filter-config

Command Mode

Global Configuration

Default

none

Usage

Use this command to display the SNMP filtering configuration:

```
MC3200(15)# show snmp-filter-config
SNMP Filtering Parameters
```

```
AP-Discovered table : on
AP-Assigned table : off
AP-Neighbor table : off
AP-Neighbor detail table : off
MC3200(15)#
```

Related Commands

[snmp-filter-config](#) on page 776

16 Station Commands

The commands contained in this chapter show information about station (client) connections:

- [*associated-station-max-idle-period*](#) on page 793
- [*no station*](#) on page 794
- [*show ap-assigned*](#) on page 795
- [*show dot11 associations*](#) on page 797
- [*show dot11 statistics client-traffic*](#) on page 799
- [*show static-station*](#) on page 802
- [*show station-log-config*](#) on page 803
- [*show station commands*](#) on page 805
- [*show station 802.11*](#) on page 809
- [*show station all*](#) on page 811
- [*show station counter*](#) on page 813
- [*show station details*](#) on page 815
- [*show station general*](#) on page 819
- [*show station mac-address*](#) on page 822
- [*show station multiple-ip*](#) on page 824
- [*show station network*](#) on page 825
- [*show station security*](#) on page 828
- [*show statistics station-per-ap*](#) on page 831
- [*show statistics top10-station-problem*](#) on page 833
- [*show statistics top10-station-talker*](#) on page 835
- [*show topostaap*](#) on page 837
- [*show topostation*](#) on page 838
- [*station-aging-out-interval*](#) on page 841
- [*station-aging-out-interval*](#) on page 841
- [*station-log*](#) on page 843

- [\(station-log\) enable](#) **on page 846**
- [\(station-log\) filelog](#) **on page 847**
- [\(station-log\) syslog](#) **on page 848**
- [\(station-log\) event id](#) **on page 849**
- [\(station-log\) event severity](#) **on page 851**
- [\(station-log\) show filters](#) **on page 853**
- [station-log show](#) **on page 855**

associated-station-max-idle-period

Configure the associated station max idle period in seconds.

Syntax

associated-station-max-idle-period <value>

value

Enter the maximum idle period for the associated station in seconds (30-86400)

Command Mode

Global configuration

Default

None

Usage

Examples

```
controller# configure terminal
controller(config)# associated-station-max-idle-period 10
```

Related Commands

no station

Deauths (deletes) the associated station from an access point.

Syntax

no station [*MAC_address*]

Command Mode

Global Configuration mode

Default

None

Usage

Deletes an associated station from its access point by sending a de-auth message to the station, forcing it off the ESS. This command is helpful for debugging connectivity issues.

Examples

The following command deletes the station information from an access points:

```
controller# no station 00:40:96:a3:b2:95
```

Related Commands

- [show station details on page 815](#)
- [show station all on page 811](#)
- [show station details on page 815](#)
- [show station counter on page 813](#)
- [show station general on page 819](#)
- [show station network on page 825](#)
- [show station security on page 828](#)

show ap-assigned

Displays assigned station information for one or more access points.

Syntax `show ap-assigned <MAC-address>`

Command Mode EXEC

Default None

Usage Displays station information for access points, including ID, MAC address, ESSID, etc. Executing the command without an argument presents a list of MAC addresses. Executing the command with the optional MAC address arguments presents detailed station information for that station.

Examples The following command shows station information for access points:

```
controller# show ap-assigned
Assigned Stations(4 entries)

AP ID Client MAC    Type    SSID      State  Encrypt Pkts Rx  Pkts Tx  Last
Prev  Curr RF  Band AP Name

2      00:02:6f:20:9a:00 STATION mwf-wpa  ASSOCIATED
TKIP   34      19      00d:00h:02m:01s 188   188   802.11a #2-2F-Sw-208
2      00:02:6f:20:9a:01 STATION mwf-wpa  ASSOCIATED
TKIP   34      19      00d:00h:02m:01s 188   188   802.11a #2-2F-Sw-208
2      00:02:6f:20:9a:02 STATION mwf-wpa  ASSOCIATED
TKIP   35      17      00d:00h:02m:01s 188   188   802.11a #2-2F-Sw-208
2      00:02:6f:20:9a:03 STATION mwf-wpa  ASSOCIATED
TKIP   34      17      00d:00h:02m:01s 188   188   802.11a #2-2F-Sw-208
Assigned Stations(4 entries)
```

The following command show the station information for the specified MAC address:

```
forti-wifi# show ap-assigned 00:40:96:a3:b2:95
Assigned Stations
```

AP ID : 3
Client MAC : 00:40:96:a3:b2:95
Type : STATION
ESSID : forti-esspeap
Association State : ASSOCIATED
Key Type : none
Packets Received : 555
Packets Sent : 304
Last Activity : 0d:0h:0m:1s
Previous RSSI : 36
Current RSSI : 30
RF Band :802.11bg
AP Name : QA

Related Commands

- [*show dot11 associations*](#) **on page 797**
- [*show dot11 statistics client-traffic*](#) **on page 799**
- [*show station all*](#) **on page 811**
- [*show station details*](#) **on page 815**
- [*show station counter*](#) **on page 813**
- [*show station general*](#) **on page 819**
- [*show station network*](#) **on page 825**
- [*show station security*](#) **on page 828**

show dot11 associations

Displays the stations seen by the system.

Syntax `show dot11 associations`

Command Mode EXEC

Default None

Usage Displays various station information, including MAC Address, availability, access point name, L2 and L3 broadcast information.

Examples The following command displays the stations seen by the system:

```
default# show dot11 associations
```

MAC Address	IP Type	AP Name	L2 Mode	L3 Mode	Authenticated
User Name	Tag	Client IP			
00:12:f0:54:a2:56	DHCP	11-Skim	wpa2-psk	clear	
0	192.168.34.21				
00:13:e8:83:27:3f	Discovered	11-Skim	wpa2-psk	clear	
0	192.168.34.116				
00:16:6f:0d:59:4d	DHCP	9-Exit-Stairs-D	wpa-psk	clear	
0	192.168.34.89				
00:16:6f:0e:18:cd	DHCP	1-ops-Kshiomoto	wpa2-psk	clear	
0	192.168.34.42				
00:16:6f:24:7f:98	Discovered	11-Skim	wpa2-psk	clear	
0	192.168.34.78				
00:18:de:bd:d0:04	Discovered	11-Skim	wpa2-psk	clear	
0	192.168.34.43				
00:19:e3:06:2c:d3	Discovered	11-Skim	wpa2-psk	clear	
0	192.168.34.86				
00:1a:6b:1d:9e:09	DHCP	1-ops-Kshiomoto	wpa2-psk	clear	
0	192.168.34.58				
00:1b:2f:c5:a5:24	DHCP	1-ops-Kshiomoto	clear	clear	
20	192.168.37.60				

```
00:1b:77:8d:75:13 DHCP      1-ops-Kshiomoto wpa2-psk clear
0    192.168.34.103
00:1b:77:95:94:79 DHCP      11-Skim        wpa2-psk clear
0    192.168.34.59
00:1b:77:95:a9:94 DHCP      29-Keith       wpa-psk  clear
0    192.168.34.44
00:1b:77:9a:63:4a DHCP      11-Skim        wpa2-psk clear
0    192.168.34.41
00:1c:bf:04:30:0e DHCP      11-Skim        wpa2-psk clear
0    192.168.34.77
00:1c:bf:25:73:6c DHCP      27-Ihab        wpa2-psk clear
0    192.168.34.54
00:40:96:a9:21:71 DHCP      10-Kaushik     wpa2-psk clear
0    192.168.34.106
```

Station Table(16 entries)

MAC Address		Availability	Client IP	IP Address Type	AP Name
L2 Mode	L3 Mode	Authenticated	User Name	Tag	
00:02:6f:20:00:00	Online		192.168.10.190	Discovered	#2-2F-Sw-
208	wpa-psk	clear		0	
00:02:6f:20:00:01	Online		192.168.10.191	Discovered	#2-2F-Sw-
208	wpa-psk	clear		0	
00:02:6f:20:00:02	Online		192.168.10.192	Discovered	#2-2F-Sw-
208	wpa-psk	clear			

Station Table(3 entries)

default#

Related
Commands

- [show ap-assigned on page 795](#)
- [show dot11 statistics client-traffic on page 799](#)
- [show station 802.11 on page 809](#)
- [show station all on page 811](#)
- [show station details on page 815](#)
- [show station counter on page 813](#)
- [show station general on page 819](#)
- [show station network on page 825](#)
- [show station security on page 828](#)

show dot11 statistics client-traffic

Displays station statistics.

Syntax

`show dot11 statistics client-traffic <ap_MAC_address>`

ap_MAC-address Specifies the station's MAC address to display additional client traffic statistics.

Command Mode

EXEC

Default

NA

Examples

The following command displays station statistics.

```
controller# show dot11 statistics client-traffic
Station Statistics
```

MAC Address	DHCP Req	AddrChg	VolHandoff	InvHandoff
00:0c:30:be:f7:c0 0		0	1	0
00:0c:85:76:35:ea 0		0	1	0
00:0c:85:e7:bf:20 0		0	4	0
00:20:a6:4c:40:1e 1		1	1	0
00:20:e0:98:10:92 0		1	2	0
00:40:96:40:ab:ae 0		1	4	0
00:40:96:49:40:ff 0		1	1	0
00:40:96:52:27:52 0		1	1	0

controller#

[Table 7](#) on page 800 describes the fields in `show dot11 statistics client-traffic` output.

TABLE 7: *Output for show dot11 statistics client-traffic*

Field	Description
MAC Address	Station MAC address.
DHCP Request Count	Number of times a client requested an IP address while connected to the Fortinet WLAN.
Address Change Count	Number of times a client IP address changed.
Voluntary Handoff Count	Number of times the Fortinet WLAN has changed AP associations to improve the client connection.
Involuntary Handoff Count	Number of times a client initiates an association to a different BSSID.

The following command displays specific statistics for the station at MAC address 00:0e:35:09:5d:5e.

```
controller# show dot11 statistics client-traffic 00:0e:35:09:5d:5e
Station Statistics
MAC Address                : 00:0e:35:09:5d:5e
DHCP Request Count         : 1
Address Change Count       : 1
Voluntary Handoff Count    : 12
Involuntary Handoff Count  : 0
QoS Active Flow Count      : 0
QoS Pending Flow Count     : 0
SIP Video Reserved Bandwidth : 0
SIP Video Bandwidth        : 0
SIP Video Flow Count       : 0
SIP Audio Reserved Bandwidth : 0
SIP Audio Bandwidth        : 0
SIP Audio Flow Count       : 0
H.323 Video Reserved Bandwidth : 0
H.323 Video Bandwidth      : 0
H.323 Video Flow Count     : 0
H.323 Audio Reserved Bandwidth : 0
H.323 Audio Bandwidth      : 0
```

H.323 Audio Flow Count : 0
SCCP Video Reserved Bandwidth : 0
SCCP Video Bandwidth : 0
SCCP Video Flow Count : 0
SCCP Audio Reserved Bandwidth : 0
SCCP Audio Bandwidth : 0
SCCP Audio Flow Count : 0

Related Commands

- [*show dot11 associations on page 797*](#)
- [*show ap-assigned on page 795*](#)
- [*show station 802.11 on page 809*](#)

show static-station

Displays the static stations.

Syntax `show static-station`

Command Mode Privileged EXEC

Default NA

Usage When a station connects through static-ip address and does not send any upstream packets, the controller will not have stations IP address information in its database. Due to this, the controller will not be able to send any downstream packet to that station. In order to avoid this situation, the station's IP details are entered manual in the controller using the command [station-aging-out-interval](#) **on page 841**. This command (show static-station) lists those stations.

Examples `ramecntrl# configure terminal`
`ramecntrl(config)# static-station 00:10:20:30:40:50`
`ramecntrl(config-static-station)# ip-address 1.1.1.1`
`ramecntrl# sh static-station`

MAC Address	Client IP (V4)
00:10:20:30:40:50	1.1.1.1

Static Station Table(1 entry)

Related Commands [station-aging-out-interval](#) **on page 841**

show station-log-config

Displays the station logging configuration for both the station filelog and syslog.

Syntax `show station-log-config`

Command Mode Privileged EXEC

Default Disabled

Usage Use this command to display the station logging configuration for both the filelog and syslog.

Example

```
ramecntrl# show station-log-config
syslog off
filelog off
ramecntrl# configure terminal
ramecntrl(config)# station-log
ramecntrl(config-station-log)# ?
do                               Executes an IOSCLI command.
end                               Save changes, and return to privileged EXEC mode.
exit                             Save changes, and return to global configuration
mode.
filelog                           Configure the filelog mode for the station log.
syslog                           Configure the syslog mode for the station log.
ramecntrl(config-station-log)# filelog on
ramecntrl(config-station-log)# syslog on
ramecntrl(config-station-log)# exit
ramecntrl(config)# exit
ramecntrl# sh station-log-config
syslog on
filelog on
ramecntrl#
station-log
```

filelog on
syslog on

Related Commands

- [station-log](#) on page 843
- [\(station-log\) filelog](#) on page 847

show station commands

The [show station details on page 815](#) command existed before, but now more show station commands have been added:

- [show station on page 807](#)
- [show station 802.11 on page 809](#)
- [show station all on page 811](#)
- [show station mac-address on page 822](#)
- [show station counter on page 813](#)
- [show station general on page 819](#)
- [show station network on page 825](#)
- [show station security on page 828](#)

Disconnected Stations has been added to the output of the command **show station all**. Use different versions of the show station command to see different output as described in the table below.

I want to see...	Use this command...
MAC Address, IP Type, APID AP Name, L2 Mode, L3 Mode, Authenticated User Name, Tag, RF Band, Client IP, Disconnected Stations that have not aged out yet	show station
802.11 stations' MAC Address, APID, AP Name, ESSID, BSSID, RF Band, TxThx, RxThx, RSSI Loss, %, CH-Util, and Disconnected Stations that have not aged out yet	show station 802.11
All stations, including ones that were dropped within the last 60 seconds: MAC Address, Service State, Type APID, AP Name, ESSID, BSSID, RF Band, Client IP, IP Type, Encrypt Pkts, Tx, Pkts, Rx, Disconnected Stations that have not aged out yet, Disconnected Stations	show station all
MAC Address, IP Type, APID AP Name, L2 Mode, L3 Mode, Authenticated User Name, Tag, RF Band, Client IP	show station details
MAC Address, MACFilterCnt, IPDiscCnt, Asso.Cnt Soft-HOCnt, PwrSavingTrCnt, KeyExCnt, RadiusAuthCnt, CPGuestUserCnt, Pkts Tx, Pkts Rx, TxByteCnt, RxByteCnt, Disconnected Stations that have not aged out yet	show station counter

I want to see...	Use this command...
MAC Address, Expected State, Service State, Type, Start time, Last Update time, Disconnected Stations that have not aged out yet	show station general
MAC Address, Client IP, IP Type, VLAN Name (mapped), Tag, IGMP Groups, Home Controller, Disconnected Stations that have not aged out yet	show station network
MAC Address, L2 Mode, L3 Mode, Auth. User Name, Encrypt, SessionTimeout, InactivityTimeout, Filter ID, Disconnected Stations that have not aged out yet	show station security

show station

Displays all data of all stations.

Syntax

show station all

Command Mode

Privileged EXEC

Default

The command **show station all** displays MAC Address, IP Type, APID AP Name, L2 Mode, L3 Mode, Authenticated User Name, Tag, RF Band, Client IP, and Disconnected Stations.

Usage

Use this version of the command to see this information for all stations, including stations that were dropped within the last 60 seconds: MAC Address, Service State, Type APID, AP Name, ESSID, BSSID, RF Band, Client IP, IP Type, Encrypt Pkts, Tx, Pkts, Rx, Disconnected Stations.

Example

```
controller# show station
```

Station Table

MAC Address	IP Type	AP Name	L2 Mode	L3 Mode	Authenticated
User Name	Tag	Client IP			
00:04:23:5a:b3:d0	DHCP	1-201-2F-SW	clear	clear	
0	192.168.10.122				
00:09:5b:c3:9f:32	Discovered	3-208-1F-Mktg	clear	clear	
0	192.168.10.121				
00:0d:93:7e:83:a7	DHCP	2-201-1F-CS	wpa-psk	clear	
0	fe80:0000:0000:0000:020d:93ff:fe7e:83a7				
00:0e:35:09:71:96	DHCP	9-208-2F-BoardR	wpa-psk	clear	
0	192.168.10.157				
00:0e:35:36:f1:f6	Discovered	3-208-1F-Mktg	clear	clear	
0	192.168.10.164				
00:0e:35:7f:1c:04	DHCP	1-201-2F-SW	wpa-psk	clear	
0	192.168.10.117				
00:0e:35:be:d9:dc	Unknown	6-208-2F-Hw-HiG	clear	clear	
0	0.0.0.0				

```

00:0e:9b:6f:4a:c0 DHCP 9-208-2F-BoardR wpa clear fortinet\joe
0 192.168.10.101
00:0e:9b:9a:0e:c7 Unknown 3-208-1F-Mktg clear clear
0 0.0.0.0
00:0e:9b:9a:0f:7b DHCP 6-208-2F-Hw-HiG wpa-psk clear
0 192.168.10.115
00:0e:9b:b3:25:b7 DHCP 9-208-2F-BoardR wpa-psk clear
0 192.168.10.125
00:11:24:2c:e0:88 DHCP 2-201-1F-CS wpa-psk clear
0 fe80:0000:0000:0000:0211:24ff:fe2c:e088
00:11:24:96:6d:4b DHCP 2-201-1F-CS clear clear
0 fe80:0000:0000:0000:0211:24ff:fe96:6d4b
00:12:f0:54:a2:56 DHCP 3-208-1F-Mktg wpa-psk clear
0 192.168.10.126
00:12:f0:86:1b:d7 DHCP 1-201-2F-SW clear clear
0 192.168.10.160
00:13:ce:5d:12:31 DHCP 6-208-2F-Hw-HiG wpa clear rjones
0 192.168.10.133
00:14:a4:0a:e5:3e Discovered 2-201-1F-CS wpa-psk clear
0 192.168.10.143
00:40:96:a9:23:f0 DHCP 6-208-2F-Hw-HiG wpa2 clear ksam-
path 0 192.168.10.120
00:90:96:c5:26:a0 DHCP 2-201-1F-CS clear clear
0 192.168.10.112

```

Station Table(19 entries)

Related Commands

- [show ap-assigned on page 795](#)
- [show dot11 statistics client-traffic on page 799](#)
- [show dot11 associations on page 797](#)
- [show station all on page 811](#)
- [show station details on page 815](#)
- [show station counter on page 813](#)
- [show station general on page 819](#)
- [show station network on page 825](#)
- [show station security on page 828](#)

show station 802.11

Displays 802.11 data for all stations.

Syntax

show station 802.11

Command Mode

Privileged EXEC

Default

NA

Usage

Use this version of the command to see the 802.11 stations' MAC Address, APID, AP Name, ESSID, BSSID, RF Band, TxThx, RxThx, RSSI, Loss, %, and CH-Util. The difference between this command and show station all is the added values for:

- Tx throughput
- Rx throughput
- RSSI
- Loss %
- CH-Util

Example

This example shows the help for the command, then the results.

```
Master1# show station ?
```

802.11	Displays 802.11 data of the stations.
all	Displays all data of the stations.
counter	Displays counter data of the stations.
details	Displays station details, including statistics.
general	Displays general data of the stations.
mac-address address	Displays details of the station with the given MAC s.
network	Displays network data of the stations.
security	Displays security data of the stations.

```
Master1# show station 802.11
```

```

MAC Address APID AP Name ESSID BSSID RF Band TxThru RxThru RSSI Loss ChUt1
RxR TxR Retr
00:03:2a:00:6a:0e 103 AP-103-Ha vcellclear 00:0c:e6:9a:5c:1c 802.11b 0 0 -
71 99 0 2 11 0
00:16:6f:b8:a4:61 103 AP-103-Ha vcellclear 00:0c:e6:9a:5c:1c 802.11bg 0 0
-56 0 0 0 0 0
00:16:6f:bb:4a:9c 103 AP-103-Ha vcellwpa2psk 00:0c:e6:9a:8e:ee 802.11bg
236767 7517 -45 0 1 39 45 20
00:16:ea:ed:be:14 103 AP-103-Ha vcellwpa2psk 00:0c:e6:9a:50:85
802.11an3s40 1419 627 -52 9 0 89 398 9
Master1#

```

Related Commands

- [*show ap-assigned on page 795*](#)
- [*show dot11 statistics client-traffic on page 799*](#)
- [*show dot11 associations on page 797*](#)
- [*show station on page 807*](#)
- [*show station all on page 811*](#)
- [*show station details on page 815*](#)
- [*show station counter on page 813*](#)
- [*show station general on page 819*](#)
- [*show station network on page 825*](#)
- [*show station security on page 828*](#)

show station all

Displays all data of all of the stations.

Syntax

show station all

Command Mode

Privileged EXEC

Default

The command **show station all** displays MAC Address, IP Type, APID AP Name, L2 Mode, L3 Mode, Authenticated User Name, Tag, RF Band, Client IP, and Disconnected Stations.

Usage

Use this version of the command to see this information for all stations, including stations that were dropped within the last 60 seconds: MAC Address, Service State, Type APID, AP Name, ESSID, BSSID, RF Band, Client IP, IP Type, Encrypt Pkts, Tx, Pkts, Rx, Disconnected Stations.

Example

```
Master1# show station ?
802.11          Displays 802.11 data of the stations.
all            Displays all data of the stations.
counter        Displays counter data of the stations.
details        Displays station details, including statistics.
general        Displays general data of the stations.
mac-address    Displays details of the station with the given MAC
address.
network        Displays network data of the stations.
security       Displays security data of the stations.
Master1# show station all

MAC Address Service State Type APID AP Name ESSID BSSID RF Band Client IP
IP Type Encrypt Pkts Tx
Pkts Rx Dev Type
00:03:2a:00:6a:0e associated sip 103 AP-103-Ha vcellclea 00:0c:e6:9a:5c:1c
802.11b 192.168.148.107 DHCP none 44
```

```

44 wireless
00:16:6f:b8:a4:61 associated data 103 AP-103-Ha vcellclea
00:0c:e6:9a:5c:1c 802.11bg 192.168.148.106 DHCP none 6309
9925 wireless
00:16:6f:bb:4a:9c associated data 103 AP-103-Ha vcellwpa2
00:0c:e6:9a:8e:ee 802.11bg 192.168.108.106 DHCP CCMP 37912
20613 wireless
00:16:ea:ed:be:14 associated data 103 AP-103-Ha vcellwpa2
00:0c:e6:9a:50:85 802.11an3s40 192.168.108.148 Discovered CCMP 18285
9751 wireless
00:16:ea:ed:c1:7c associated data 103 AP-103-Ha vcellwpa2
00:0c:e6:9a:50:85 802.11an3s40 192.168.108.184 DHCP CCMP 518555
2630807 wireless
00:16:ea:ed:c3:12 associated data 103 AP-103-Ha vcellclea
00:0c:e6:9a:cb:17 802.11an3s40 192.168.148.102 Discovered none 14615
14208 wireless
00:16:ea:ed:c7:e6 associated data 103 AP-103-Ha vcellwpa2
00:0c:e6:9a:50:85 802.11an3s40 192.168.108.158 Discovered CCMP 18872
10178 wireless
00:16:ea:ed:cf:7c associated data 103 AP-103-Ha vcellwpa2
00:0c:e6:9a:50:85 802.11an3s40 192.168.108.128 Discovered CCMP 17728
11442 wireless

```

Related Commands

- [*show station* on page 807](#)
- [*show station 802.11* on page 809](#)
- [*show station details* on page 815](#)
- [*show station general* on page 819](#)
- [*show station mac-address* on page 822](#)
- [*show station network* on page 825](#)
- [*show station security* on page 828](#)

show station counter

Displays counter data used for diagnostic inferences, either for all stations or just the one indicated.

Syntax

```
show station counter
show station counter mac-address <MAC address>
```

Command Mode

Privileged EXEC

Default

The command version **show station counter mac-address** displays MAC Address, IP Type, APID AP Name, L2 Mode, L3 Mode, Authenticated User Name, Tag, RF Band, Client IP.

Usage

Use this command to display various counter details of the station. The details for MAC Filter ACL Count, IP Discovery Count, Association Count, Soft Handoff Count, Power Saving Transition Count, Key Exchange Count, Radius Authentication Count, Captive Portal Guest User Count, Packets Sent, Packets Received, Transmitted Byte Count, Received Byte Count, QoS Flow Count, Voice Call Count, MAC Filter ACL Fail Count, Radius Authentication Fail Count, Key Exchange Fail Count, Captive Portal Guest User Fail Count, Decrypt Fail Count, WEP Key Index Mismatch Count, MIC Fail Count, Assign Fail Count, Packet Loss Count, Power Save Poll Frames Received Count, SW Encryption Frames Count, SW Decryption Frames Count, LRU Swap Count and Tx Failed Count by Hardware Retry Exceed counters are displayed.

Example

```
namecntrl# sh station counter
```

MAC Address	MacFilter	IPDisc	Asso.	SoftH0	PSTr	KeyEx	RadAuth
CPGuest	Pkts Tx	Pkts Rx	TxByteCnt	RxByteCnt			
00:40:96:ae:20:7a	1	1	1	0	0	1	2
154	229	51242	25604				0

Station Database Counter Table(1 entry)

```
namecntrl# sh station counter mac-address 00:40:96:ae:20:7a
```

Station Database Counter Table

MAC Address	: 00:40:96:ae:20:7a
MAC Filter ACL Count	: 1
IP Discovery Count	: 1

```

Association Count                : 1
Soft Handoff Count              : 0
Power Saving Transition Count    : 0
Key Exchange Count              : 1
Radius Authentication Count      : 2
Captive Portal Guest User Count : 0
Packets Sent                    : 154
Packets Received                : 229
Transmitted Byte Count          : 51242
Received Byte Count             : 25604
QoS Flow Count                  : 0
Voice Call Count                : 0
MAC Filter ACL Fail Count       : 0
Radius Authentication Fail Count : 0
Key Exchange Fail Count         : 0
Captive Portal Guest User Fail Count : 0
Decrypt Fail Count              : 0
WEP Key Index Mismatch Count    : 0
MIC Fail Count                  : 0
Assign Fail Count               : 0
Packet Loss Count               : 53
Power Save Poll Frames Received Count : 0
SW Encryption Frames Count      : 0
SW Decryption Frames Count      : 0
LRU Swap Count                  : 0
Tx Failed Count by Hardware Retry Exceed : 0
namecntrl#

```

Related Commands

- [*show station* on page 807](#)
- [*show station 802.11* on page 809](#)
- [*show station all* on page 811](#)
- [*show station details* on page 815](#)
- [*show station general* on page 819](#)
- [*show station mac-address* on page 822](#)
- [*show station network* on page 825](#)
- [*show station security* on page 828](#)

show station details

Displays station detail information for all stations or stations associated with the given name.
This command already existed in a previous release.

Syntax

```
show station details ip-address <IP address>
show station details mac-address <MAC address>
show station details user <user>
```

Command Mode

Privileged EXEC

Default

none

Usage

Use the **show station details** command to see a list of associated stations listed with their IP addresses or MAC addresses or users.

TABLE 8: *Output for Command show station details*

Field	Description
MAC Address	MAC address of the station.
IP Type	Method by which the IP address of the station is assigned: Static IP address assigned: Station uses a static IP address. IPv6 IP addresses show as Dynamic IP address assigned: Station uses a static IP address, which is learned from the traffic sent. DHCP: Station uses an IP address assigned by DHCP.
AP Name	Name of the access point.
L2 Mode	Layer 2 authentication used.
L3 Mode	Layer 3 authentication used.
Authenticated User Name	Authenticated user name associated with station, if used.

TABLE 8: *Output for Command show station details*

Field	Description
Tag	VLAN tag associated with the station, if it exists.
Client IP	IP address assigned to the station. IPv6 addresses display similar to fe80:0000:0000:0000:020d:93ff:fe7e:83a7 instead of a normal 4-tuple IP address.

Using keywords with the **show station** command presents additional information and statistics.

Use the keyword **mac-address** with a station's MAC address to see information about a particular station. The following information is added in this case:

Field	Description
DHCP Req	Each time a controller sees a DHCP request from a mobile client, it increases this counter.
AddrChg	Each time a controller sees a mobile client's IP change from A to B, it increases this counter.
VolHandoff	Each time a controller does a soft handoff, it increases this counter. Topology-updated must be enabled.
InvHandoff	Each time when a mobile client does a hard handoff, a controller increases this counter. Topology-updated needs to be enabled.

The IP address can appear as 0.0.0.0 in the following situations:

- Client with static IP address: After a client has associated with an access point, but before the client has sent its first packet. After the first packet is sent, the client IP address and address type appears in **show station** output.
- Client with IP address assigned by DHCP: After a client has sent a DHCP request, but before the DHCP server responds. After the DHCP server responds, the client IP address and address type appears in **show station** output.

Use the keywords **details ip-address**, **details user**, and **mac-address** to see detailed information about the station in the station table and assorted station statistics.

If a station remains inactive for 30 minutes, it is disconnected from the WLAN.

Examples

The following command displays information for associated stations.

```
controller# show station details mac-address 00:20:a6:4e:b5:9c
```

Station Table

MAC Address	IP Type	AP Name	L2 Mode	L3 Mode	Authenticated
User Name	Tag	Client IP			

00:40:96:a9:21:71	DHCP	10-Kaushik	wpa2-psk	clear	
0	192.168.34.106				

Station Statistics

MAC Address	DHCP Req	AddrChg	VolHandoff	InvHandoff
-------------	----------	---------	------------	------------

00:40:96:a9:21:71	0	0	1306	0
-------------------	---	---	------	---

Assigned AP Table for MAC address 00:40:96:a9:21:71

AP ID	Client MAC	Type	SSID	State
Encrypt	Pkts Rx	Pkts Tx	Last	AP Name
Prev	Curr	RF Band		
10	00:40:96:a9:21:71	STATION	corp-wpa2psk	ASSOCIATED
CCMP	248810	111399	00d:00h:00m:05s	-71 -66 802.11abg 10-Kau-shik

There are no QoS flows for MAC address 00:40:96:a9:21:71 (IP: 192.168.34.106)

Station Table

MAC Address	Availability	Client IP	IP Address	Type	AP Name
L2 Mode	L3 Mode	Authenticated	User Name	Tag	

00:20:a6:4e:b5:9c	Online	192.168.10.140	DHCP		#8-1F-
DemoArea-	wpa-psk	clear		0	

Station Statistics

MAC Address	DHCP Req	AddrChg	VolHandoff	InvHandoff
00:20:a6:4e:b5:9c	0	0	4	0

Assigned AP Table for MAC address 00:20:a6:4e:b5:9c

AP ID	Client MAC	Type	SSID					State
Encrypt	Pkts Rx	Pkts Tx	Last	Prev	Curr	RF Band	AP Name	
8	00:20:a6:4e:b5:9c	STATION	mwf-wpapsk					ASSOCIATED
TKIP	4377	4566	00d:00h:00m:00s	205	204	802.11g	#8-1F-DemoArea-	

There are no QoS flows for MAC address 00:20:a6:4e:b5:9c (IP: 192.168.10.140)

Related
Commands

- [show station on page 807](#)
- [show station 802.11 on page 809](#)
- [show station all on page 811](#)
- [show station counter on page 813](#)
- [show station details on page 815](#)
- [show station general on page 819](#)
- [show station mac-address on page 822](#)
- [show station network on page 825](#)
- [show station security on page 828](#)

show station general

Displays general data for all stations or for the indicated station.

Syntax

```
show station general
show station general ip-address <IP address>
show station general mac-address <MAC address>
show station general user <username>
```

Command Mode

Privileged EXEC

Default

The command version **show station** displays MAC Address, IP Type, APID AP Name, L2 Mode, L3 Mode, Authenticated User Name, Tag, RF Band, Client IP.

Usage

Use this command to see general station information.

Example

```
Master1# show station general
```

MAC Address	Expected State	Service State	Type	Start time
Last Update time				
00:03:2a:00:d7:c0	unknown	associated	data	06/16/2009
06:03:52	06/16/2009	06:30:23		
00:03:2a:00:e4:3f	unknown	associated	data	06/16/2009
06:03:52	06/16/2009	06:30:23		
00:11:24:92:40:4d	unknown	associated	data	06/16/2009
06:03:52	06/16/2009	06:30:23		
00:11:95:c2:29:1e	unknown	associated	data	06/16/2009
06:04:59	06/16/2009	06:30:23		
00:13:e8:06:cd:6b	unknown	associated	data	06/16/2009
06:03:52	06/16/2009	06:30:23		
00:16:6f:b8:d5:15	unknown	associated	data	06/16/2009
06:03:52	06/16/2009	06:30:23		
00:16:ea:88:1c:84	unknown	associated	data	06/16/2009
06:03:52	06/16/2009	06:30:23		

00:17:9a:50:d8:23 unknown	associated	data 06/16/2009
06:03:52 06/16/2009 06:30:23		
00:19:5b:03:44:93 unknown	associated	data 06/16/2009
06:03:52 06/16/2009 06:30:23		
00:19:7e:91:0a:7f unknown	associated	data 06/16/2009
06:03:52 06/16/2009 06:30:23		
00:19:7e:91:0a:89 unknown	associated	data 06/16/2009
06:08:08 06/16/2009 06:30:23		
00:1a:c1:35:84:36 unknown	associated	data 06/16/2009
06:03:52 06/16/2009 06:30:23		
00:1a:c1:35:86:96 unknown	associated	data 06/16/2009
06:03:52 06/16/2009 06:30:23		
00:1b:2f:c5:a5:1e unknown	associated	data 06/16/2009
06:03:52 06/16/2009 06:30:23		
00:1b:2f:d0:5b:8c unknown	associated	data 06/16/2009
06:03:52 06/16/2009 06:30:23		
00:1b:2f:d0:5b:90 unknown	associated	data 06/16/2009
06:03:52 06/16/2009 06:30:23		
00:1b:77:9a:61:4a unknown	associated	data 06/16/2009
06:03:52 06/16/2009 06:30:23		
00:1c:f0:9d:e3:fe unknown	associated	data 06/16/2009
06:03:52 06/16/2009 06:30:23		
00:1c:f0:9d:e4:0d unknown	associated	data 06/16/2009
06:03:52 06/16/2009 06:30:23		
00:1d:7e:0a:94:9c unknown	associated	data 06/16/2009
06:03:52 06/16/2009 06:30:23		
00:1f:e2:d8:39:92 unknown	associated	data 06/16/2009
06:03:52 06/16/2009 06:30:23		
00:20:a6:4e:c3:1b unknown	associated	data 06/16/2009
06:03:52 06/16/2009 06:30:23		
00:21:00:41:50:ce unknown	associated	data 06/16/2009
06:03:52 06/16/2009 06:30:23		
00:21:00:d7:f1:b6 unknown	associated	data 06/16/2009
06:03:52 06/16/2009 06:30:23		
00:21:00:d7:f2:b2 unknown	associated	data 06/16/2009
06:03:52 06/16/2009 06:30:23		
00:21:5c:08:ec:c7 unknown	associated	data 06/16/2009
06:03:52 06/16/2009 06:30:23		
00:21:5d:45:fa:12 unknown	associated	data 06/16/2009
06:03:52 06/16/2009 06:30:23		
00:22:68:a0:f0:3b unknown	associated	data 06/16/2009
06:03:52 06/16/2009 06:30:23		

00:40:96:b4:12:c2 unknown associated data 06/16/2009
06:03:52 06/16/2009 06:30:23

Station Database General Table(29 entries)

Master1#

Related Commands

- [*show station on page 807*](#)
- [*show station 802.11 on page 809*](#)
- [*show station all on page 811*](#)
- [*show station counter on page 813*](#)
- [*show station details on page 815*](#)
- [*show station mac-address on page 822*](#)
- [*show station network on page 825*](#)
- [*show station security on page 828*](#)

show station mac-address

Displays all data for the station with the named MAC address.

Syntax

show station <MAC address>

Command Mode

Privileged EXEC

Default

NA

Usage

The command version displays only a station with this MAC Address.

Example

```
Master1# show station ?
802.11          Displays 802.11 data of the stations.
all             Displays all data of the stations.
counter        Displays counter data of the stations.
details        Displays station details, including statistics.
general        Displays general data of the stations.
mac-address    Displays details of the station with the given MAC
address.
network        Displays network data of the stations.
security       Displays security data of the stations.
controller# show station mac-address 00:20:a6:4e:b5:9c
Station Table

MAC Address      : 00:20:a6:4e:b5:9c
IP Address Type  : DHCP
AP ID            : 10
AP Name          : 10-Kaushik
L2 Security State : wpa2-psk
L3 Security State : clear
Authenticated User Name :
VLAN Name       :
```

Tag : 0
RF Band : unknown
Client IP : 192.168.34.106
Availability Status : Online
Description :
Client IP : 192.168.10.140
IP Address Type : DHCP
AP ID : 8
AP Name : #8-1F-DemoArea-201
L2 Security State : wpa-psk
L3 Security State : clear
Authenticated User Name :
VLAN Name :
Tag : 0
RF Band : 802.11g

Related Commands

- [*show station on page 807*](#)
- [*show station 802.11 on page 809*](#)
- [*show station all on page 811*](#)
- [*show station counter on page 813*](#)
- [*show station details on page 815*](#)
- [*show station general on page 819*](#)
- [*show station mac-address on page 822*](#)
- [*show station network on page 825*](#)
- [*show station security on page 828*](#)

show station multiple-ip

Displays all stations utilizing multiple IP addresses on a single MAC.

Syntax `show station multiple-ip`

Command Mode Privileged EXEC

Default NA

Usage Use this command when you wish to determine which IP addresses are in use for a station that is running virtualized environments on a single adapter.

Example

```
Master1# show station ?
802.11          Displays 802.11 data of the stations.
all             Displays all data of the stations.
counter        Displays counter data of the stations.
details        Displays station details, including statistics.
general        Displays general data of the stations.
mac-address    Displays details of the station with the given MAC
address.
multiple-ip    Displays multiple ip addresses of the stations.
network        Displays network data of the stations.
security       Displays security data of the stations.
```

show station network

Displays network data for all stations or for the indicated station.

Syntax

```
show station network
show station network ip-address <IP address>
show station network mac-address <MAC address>
show station network user <username>
```

Command Mode

Privileged EXEC

Default

The command version **show station** displays MAC Address, IP Type, APID AP Name, L2 Mode, L3 Mode, Authenticated User Name, Tag, RF Band, Client IP.

Usage

Use this command to see station network information.

Example

This example shows a station network.

```
Master1# show station network
```

MAC Address Groups	Client IP Home Controller	IP Type	VLAN Name	Tag	IGMP
00:03:2a:00:d7:c0 0	192.168.106.139	DHCP	106	106	0
00:03:2a:00:e4:3f 0	192.168.106.140	DHCP	106	106	0
00:11:24:92:40:4d 0	192.168.106.137	DHCP	106	106	0
00:11:95:c2:29:1e 0	192.168.106.141	DHCP	106	106	0
00:13:e8:06:cd:6b 0	192.168.108.104	DHCP	108	108	0
00:16:6f:b8:d5:15 0	192.168.108.106	DHCP	108	108	0
00:16:ea:88:1c:84 0	192.168.108.116	DHCP	108	108	0

00:17:9a:50:d8:23	192.168.106.179	DHCP	106	106	0
0					
00:19:5b:03:44:93	192.168.106.174	Discovered	106	106	0
0					
00:19:7e:91:0a:7f	0.0.0.0	Unknown		0	0
0					
00:19:7e:91:0a:89	192.168.108.108	DHCP	108	108	0
0					
00:1a:c1:35:84:36	192.168.103.102	DHCP	VLAN103	103	0
0					
00:1a:c1:35:86:96	192.168.103.100	DHCP	VLAN103	103	0
0					
00:1b:2f:c5:a5:1e	192.168.106.181	DHCP	106	106	0
0					
00:1b:2f:d0:5b:8c	192.168.77.100	Discovered		4096	0
0					
00:1b:2f:d0:5b:90	192.168.108.123	DHCP	108	108	0
0					
00:1b:77:9a:61:4a	0.0.0.0	Unknown	VLAN103	103	0
0					
00:1c:f0:9d:e3:fe	192.168.103.104	DHCP	VLAN103	103	0
0					
00:1c:f0:9d:e4:0d	10.101.66.6	DHCP		0	0
0					
00:1d:7e:0a:94:9c	192.168.108.107	DHCP	108	108	0
0					
00:1f:e2:d8:39:92	192.168.108.115	DHCP	108	108	0
0					
00:20:a6:4e:c3:1b	192.168.106.195	DHCP	106	106	0
0					
00:21:00:41:50:ce	192.168.108.103	Discovered	108	108	0
0					
00:21:00:d7:f1:b6	192.168.106.123	Discovered	106	106	0
0					
00:21:00:d7:f2:b2	0.0.0.0	Unknown		0	0
0					
00:21:5c:08:ec:c7	0.0.0.0	Unknown	VLAN103	103	0
0					
00:21:5d:45:fa:12	10.101.66.2	Discovered		0	0
0					
00:22:68:a0:f0:3b	192.168.108.109	DHCP	108	108	0
0					

00:40:96:b4:12:c2 192.168.108.105 DHCP 108 108 0
0

Station Database Network Table(29 entries)

**Related
Commands**

- [*show ap-assigned on page 795*](#)
- [*show dot11 statistics client-traffic on page 799*](#)
- [*show station 802.11 on page 809*](#)
- [*show station all on page 811*](#)
- [*show station details on page 815*](#)
- [*show station counter on page 813*](#)
- [*show station general on page 819*](#)
- [*show station security on page 828*](#)

show station security

Displays security data for all stations or just for the indicated station.

Syntax

```
show station security
show station security ip-address <IP address>
show station security mac-address <MAC address>
show station security user <username>
```

Command Mode

Privileged EXEC mode

Default

The command version **show station** displays MAC Address, IP Type, APID AP Name, L2 Mode, L3 Mode, Authenticated User Name, Tag, RF Band, Client IP.

Usage

Examples

```
Master1# show station security
```

MAC Address	L2 Mode	L3 Mode	Auth. User Name
Encrypt SessionTimeout	InactivityTimeout	Filter ID	
00:03:2a:00:d7:c0	clear	clear	none
0	0		
00:03:2a:00:e4:3f	clear	clear	none
0	0		
00:11:24:92:40:4d	clear	clear	none
0	0		
00:11:95:c2:29:1e	clear	clear	none
0	0		
00:13:e8:06:cd:6b	wpa2-psk	clear	CCMP
0	0		
00:16:6f:b8:d5:15	wpa2-psk	clear	CCMP
0	0		
00:16:ea:88:1c:84	wpa2-psk	clear	CCMP
0	0		
00:17:9a:50:d8:23	clear	clear	none
0	0		

00:19:5b:03:44:93	clear	clear	none
0	0		
00:19:7e:91:0a:7f	wpa2-psk	clear	CCMP
0	0		
00:19:7e:91:0a:89	wpa2-psk	clear	CCMP
0	0		
00:1a:c1:35:84:36	wep	clear	WEP
0	0		
00:1a:c1:35:86:96	wep	clear	WEP
0	0		
00:1b:2f:c5:a5:1e	clear	clear	none
0	0		
00:1b:2f:d0:5b:8c	wpa2	clear	CCMP
0	0		
00:1b:2f:d0:5b:90	wpa2-psk	clear	CCMP
0	0		
00:1b:77:9a:61:4a	wep	clear	WEP
0	0		
00:1c:f0:9d:e3:fe	wpa-psk	clear	TKIP
0	0		
00:1c:f0:9d:e4:0d	wpa-psk	clear	TKIP
0	0		
00:1d:7e:0a:94:9c	wpa2-psk	clear	CCMP
0	0		
00:1f:e2:d8:39:92	wpa2-psk	clear	CCMP
0	0		
00:20:a6:4e:c3:1b	clear	clear	none
0	0		
00:21:00:41:50:ce	wpa2-psk	clear	CCMP
0	0		
00:21:00:d7:f1:b6	clear	clear	none
0	0		
00:21:00:d7:f2:b2	wpa-psk-in-progress	clear	
none	0	0	
00:21:5c:08:ec:c7	wep	clear	WEP
0	0		
00:21:5d:45:fa:12	wpa-psk	clear	TKIP
0	0		
00:22:68:a0:f0:3b	wpa2-psk-in-progress	clear	
CCMP	0	0	
00:40:96:b4:12:c2	wpa2-psk	clear	CCMP
0	0		

Station Database General Table(29 entries)

Related Commands

- [*show ap-assigned*](#) **on page 795**
- [*show dot11 statistics client-traffic*](#) **on page 799**
- [*show station 802.11*](#) **on page 809**
- [*show station all*](#) **on page 811**
- [*show station details*](#) **on page 815**
- [*show station counter*](#) **on page 813**
- [*show station general*](#) **on page 819**
- [*show station network*](#) **on page 825**

show statistics station-per-ap

Displays station statistics per access point.

Syntax `show statistics station-per-ap <ap-id>`

Command Mode EXEC

Default None

Usage Use the `show statistics station-per-ap` command to see station statistics on a per access-point basis. By default, all station statistics for all access points are shown. To see station statistics for one access point, specify the access point's identification number when issuing the command.

Examples The following (abbreviated) command display shows the station statistics for all access points.

```
controller# show statistics station-per-ap
AP  AP-Name  If  Station-MAC  Station-IP  SSID  Rx-
packets  Tx-packets  WEP-errorsEncryptionErr

2    #2-2F-Sw- 2    00:02:6f:20:00:33  0.0.0.0      mwf-wpa
1138      1134      0

2    #2-2F-Sw- 2    00:02:6f:20:00:32  0.0.0.0      mwf-wpa      996
988      0

2    #2-2F-Sw- 2    00:02:6f:20:00:31  0.0.0.0      mwf-wpa
1142      1132      0
controller#
```

TABLE 9: *Output for show statistic station-per-ap*

Field	Description
AP	Unique ID number of the access point to which the station is currently communicating.
AP-Name	Name of the access point to which the station is currently communicating.
If	AP interface number.
Station-MAC	MAC address of the station.
Station-IP	IP address of the station.
SSID	ESSID to which the station is associated.
Rx-packets	Total number of packets received by the access point from the station.
Tx-packets	Total number of packets transmitted to the station from the access point.
WEP-errorsEncryptionErr	Number of encryption errors per minute. Encryption errors are most likely to occur when stations have not executed the 802.1x protocol successfully during session initiation or rekey period.

**Related
Commands**

- [show ap-assigned on page 795](#)
- [show dot11 statistics client-traffic on page 799](#)
- [show station 802.11 on page 809](#)
- [show station all on page 811](#)
- [show station details on page 815](#)
- [show station counter on page 813](#)
- [show station general on page 819](#)
- [show station network on page 825](#)
- [show station security on page 828](#)

show statistics top10-station-problem

Displays the top ten stations with the highest number of WEP errors per minute, with a minimum of 10 WEP errors per minute.

Syntax `show statistics top10-station-problem`

Command Mode Privileged EXEC

Default NA

Usage Use the `show statistics top10-station-problem` command to see the top ten stations with the highest number of WEP errors per minute, with a minimum of 10 WEP errors per minute. WEP errors are most likely to occur when stations have not executed the 802.1x protocol successfully during session initiation or rekey period.

Examples The following command displays the top ten stations with the highest number of WEP errors per minute.

```
controller# show statistics top10-station-problem
```

AP	AP Name	If	Station MAC	Station IP	WEP Errors/min
11	11-Skim	1	00:1b:77:95:ab:81	0.0.0.0	105588
11	11-Skim	1	00:18:de:bd:d0:04	192.168.34.43	69757
1	1-ops-Ksh	1	00:1b:77:8d:75:13	192.168.34.103	58694
11	11-Skim	1	00:1c:bf:04:30:0e	192.168.34.77	51486
10	10-Kaushi	1	00:1b:77:50:b1:2a	0.0.0.0	33294
10	10-Kaushi	1	00:1c:bf:ae:4b:01	0.0.0.0	25154
29	29-Keith	1	00:1b:77:95:a9:94	192.168.34.44	18897
1	1-ops-Ksh	1	00:13:02:28:f4:9a	0.0.0.0	14929
11	11-Skim	1	00:1b:77:95:94:79	192.168.34.59	8140
9	9-Exit-St	1	00:13:02:88:6a:e2	0.0.0.0	7304

Top 10 station problem statistics(10)

[Table 10](#) on page 834 describes the fields for the **show statistics top10-station-problem** command.

TABLE 10: *Output for show statistics top10-station-problem*

Field	Description
AP	Unique ID number of the access point.
AP Name	Name of the access point to which the station is associated.
If	Interface number of the AP.
Station MAC	MAC address of the station.
Station IP	IP address of the station.
WEP Errors/Minute	Cumulative number of WEP errors that have occurred during the last minute.

**Related
Commands**

[show statistics top10-station-talker](#) on page 835

show statistics top10-station-talker

Displays the 10 most active stations, based on the sum of transmission and reception packet rates per minute during the last polling period.

Syntax `show statistics top10-station-talker`

Command Mode Privileged EXEC

Default NA

Usage Use the `show statistics top10-station-talker` command to display the 10 most active stations, based on the sum of transmission and reception packet rates per minute during the last polling period since the last reset. The top talker stations table shows activity based on the number of frames per minute, not actual bytes transmitted or airtime consumed.

Examples The following command displays the most active stations.

```
controller# show statistics top10-station-talker
```

AP	AP Name	If	Station MAC	Station IP	Rx Packets/min	Tx Packets/min
10	#10-1F-Mk 1	00:0e:35:09:5d:5e	192.168.10.125	370	400	
8	#8-1F-Dem 1	00:05:4e:40:6f:46	192.168.10.141	357	347	
6	#6-1F-CS- 1	00:0e:35:5f:f0:29	0.0.0.0	359	328	
10	#10-1F-Mk 1	00:12:f0:0f:23:cd	0.0.0.0	259	304	
10	#10-1F-Mk 1	00:0e:35:5f:f0:29	0.0.0.0	300	244	
10	#10-1F-Mk 2	00:09:5b:a3:c2:fd	192.168.10.130	246	237	
2	#2-2F-Sw- 2	00:02:6f:20:00:16	0.0.0.0	227	227	
2	#2-2F-Sw- 2	00:02:6f:20:00:33	0.0.0.0	227	226	
2	#2-2F-Sw- 2	00:02:6f:20:00:31	0.0.0.0	228	226	
2	#2-2F-Sw- 2	00:02:6f:20:00:3a	0.0.0.0	227	226	

Top 10 station talker statistics request(10)

```
controller#
```

[Table 11](#) on page 836 describes the fields of the `show statistics top10-station-talker` output.

TABLE 11: *Output for show statistics top10-station-talker*

Field	Description
AP	Unique ID number of the access point.
AP Name	Name of the access point to which the station is currently communicating.
If	Interface number of the AP.
Station MAC	MAC address of the station.
Station IP	IP address of the station.
Rx Packets/min	Number of packets received since the last reset during the last polling period.
Tx packets/min	Number of packets transmitted since the last reset during the last polling period.

**Related
Commands**

[show statistics top10-station-problem](#) on page 833

show topostaap

Displays the station/AP edge records in the system.

Syntax `show topostaap`

Command Mode Privileged EXEC

Default None

Usage This command displays the station/AP edge records in the system.

Examples controller# `show topostaap`

Station MAC Address	AP ID	AP Name	Assigned	RSSI
00:0d:93:82:da:b3	1	AP-1	on	36
00:40:96:40:fa:eb	1	AP-1	on	28
00:40:96:51:c6:40	1	AP-1	on	0

Related Commands

show topostation

Displays information about stations currently assigned to access points.

Syntax `show topostation`

Command Mode Privileged EXEC

Default None

Usage Use the `show topostation` command to see information about stations currently assigned to access points (from the station point of view). Only stations that are a part of FortiWLC (SD) are shown. Use the `show ap-discovered` command to see other stations.

Examples The following command displays stations that are part of FortiWLC (SD):

```
controller# show topostation
MAC Address      AP   AP Name      Last Handoff Time      State
BSSID            MSSID
00:12:f0:54:a2:56 11   11-Skim      2008/03/12 11:50:21     ASSOCIATED
00:12:F2:40:61:2f 00:00:00:00:00:00
00:13:e8:83:27:3f 11   11-Skim      2008/03/12 11:29:53     ASSOCIATED
00:12:F2:40:61:2f 00:00:00:00:00:00
00:13:e8:dd:17:57 8     8-Saro       2008/03/12 10:41:53     ASSOCIATED
00:12:F2:40:61:2f 00:00:00:00:00:00

      Stations Topology(3 entries)
MAC Address      AP   AP Name      Last Handoff Time      State
BSSID            MSSID

00:12:f0:54:a2:56 11   11-Skim      2008/03/12 11:50:21     ASSOCIATED
00:12:F2:40:61:2f 00:00:00:00:00:00
00:13:e8:83:27:3f 11   11-Skim      2008/03/12 11:29:53     ASSOCIATED
00:12:F2:40:61:2f 00:00:00:00:00:00
00:13:e8:dd:17:57 8     8-Saro       2008/03/12 10:41:53     ASSOCIATED
00:12:F2:40:61:2f 00:00:00:00:00:00

      Stations Topology(3 entries)
Last Handoff Time      State      MAC Address      AP   AP Name
                        BSSID
```

00:02:c7:34:48:90 8	#8-1F-DemoArea-	2005/08/09 08:47:19	ASSOCIATED
00:0c:e6:02:07:2f			
00:03:2a:00:6a:80 3	#3-2F-Exec-201	2005/08/09 14:59:04	ASSOCIATED
00:0c:e6:44:08:eb			
00:03:2a:00:6b:a6 8	#8-1F-DemoArea-	2005/08/09 15:48:26	ASSOCIATED
00:0c:e6:44:08:eb			

Stations Topology(3 entries)

controller#

**Related
Commands**

- [show ap-discovered on page 632](#)
- [show ap-assigned on page 795](#)
- [show dot11 statistics client-traffic on page 799](#)
- [show station 802.11 on page 809](#)
- [show station all on page 811](#)
- [show station details on page 815](#)
- [show station counter on page 813](#)
- [show station general on page 819](#)
- [show station network on page 825](#)
- [show station security on page 828](#)

static-station

Sets a static IP for a station that is unable to use DHCP.

Syntax

```
static-station MAC_address  
    ip_address ip_address  
no static-station MAC_address
```

Command Mode

Global Configuration mode

Default

None

Usage

Use this command to set a static IP address for a station that is unable to use DHCP and therefore doesn't transmit any upstream packets. For those clients, it is not possible to automatically learn the IP to MAC-address mapping. This command provides a way to manually create an IP to MAC mapping.

Entering the MAC address of the station enters config-static-station submode, where the ip-address command is given.

Use the no form of the command to remove a MAC address to IP address mapping for a station.

Examples

Here IP address 172.172.172.10 is assigned to the station with MAC address 00:00:04:23:55:15:

```
controller (config)# static-station 00:00:04:23:55:15  
controller(config-static-station)# ip-address 172.172.172.10
```

To remove a static station assignment, use the following example:

```
controller (config)# no static-station 00:00:04:23:55:15
```

station-aging-out-interval

Sets how long the station entry remains in the station table in E(z)RF Network Manager after the station has left the system.

Syntax

station-aging-out-interval <minutes>

Command Mode

Global Configuration mode

Default

The default value is set to 0 which means the station entry for the counters is removed as soon as the wncreg removes the entry.

Usage

This command was introduced in release 3.6.1 and is basically used for show station counters which includes (802.11, all, counter, details, general, network, security). The default value is set to "0" which means the station entry for the counters removed as soon as the wncreg removes the entry. **station-aging -out-interval** sets how long the station entry remains in the station table in E(z)RF Network Manager after the station has left the system. The rationale behind this parameter is that the output of the command **show station** contains useful information for debugging and other purposes. Prior to release 3.6.1, a station entry was removed once the station left the network; if a problem was reported after a station was gone, there was little left in the system to debug the station's problem. Indicate a number of minutes from 1 and 65535. When set to 0 (zero) the station entry for the counters is removed as soon as the wncreg removes the entry. This zero default is the same setting used in older FortiWLC (SD) versions where the parameter did not exist.

The values represents "Minutes" so when the value is set to 60 the wncagent keeps the station counter details (which is all the counters) for 60 more mins after the station is gone out of the network. You can set the timer to any value between 1 and 65535. Output of the command **show controller** shows the station aging out time.

Example

This example sets the aging out interval to 60 and then checks the setting with the command **show controller**.

```
InteropLab(config)# station-aging-out-interval ?
<0-65535>          Enter the station aging out interval(minute) between
1 and 65535, or 0 to disable.
InteropLab(config)# station-aging-out-interval 60
InteropLab(config)# exit
```

```

InteropLab # sh controller
Global Controller Parameters
Controller ID                : 1
Description                  : controller
Host Name                    : Engg-wifi-Main
Uptime                       : 01d:10h:44m:23s
Location                     :
Contact                      :
Operational State            : Enabled
Availability Status           : Online
Alarm State                   : Critical
Automatic AP Upgrade         : off
Virtual IP Address           : 10.101.64.100
Virtual Netmask               : 255.255.192.0
Default Gateway               : 10.101.64.1
DHCP Server                   : 192.168.101.250
Statistics Polling Period (seconds)/0 disable Polling : 60
Audit Polling Period (seconds)/0 disable Polling      : 60
Software Version              : 4.0-38
Network Device Id             : 00:00:50:51:e6:cc
System Id                     : DC89C8D202DA
Default AP Init Script        :
DHCP Relay Passthrough        : on
Controller Model               : MC5000
Country Setting                : United States Of
America
Manufacturing Serial #        : N/A
Management by wireless stations : on
Controller Index               : 10
Topology Information Update    : on
AeroScout Enable/Disable      : disable
FastPath Mode                  : on
Bonding Mode                   : dual
DFS                            : disable
Station Aging Out Period(minutes) : 60
Roaming Domain State           : disable

```

station-log

Enables debug messages for 802.11 connection.

Syntax

station-log <station MAC address>

Command Mode

Global Configuration mode

Default

None

Usage

This command gathers information about the named station, specifically 802.11 Probe, Auth, Assoc, Deauth, Disassoc etc.

Examples

```
default# station-log ?
<CR>
<station_mac>          Specific station MAC you want to view.
show                   Display station log events.
default# station-log
Interactive Per-Station Event Logging Shell (enter "help" for help)
station-log> ?
```

Interactive Event Logging Shell Usage:

help, ?	This help message
exit, quit	Exit/Quit
station show	Show stations in the filter list
station add <AA:BB:CC:DD:EE:FF> MAC	Add a station to the filter list by MAC
station del <AA:BB:CC:DD:EE:FF> by MAC	Delete a station from the filter list by MAC
station del <#> by index	Delete a station from the filter list by index
station del all list	Delete all stations from the filter list

```

event show                                Show the event filter list
event <event> <dispcnd>                  Set the display condition for event
<event>

<event> may be: #ID of event, or "all"
<dispcnd> may be: "all" (!), "none"

(x) or "list" (?)
station-log> station show
The station filter list is empty!
station-log> event show ?
Event Filters
=====
Disp | ID# | Name
-----
? | 1 | IP Address Discovered
? | 2 | DHCP
? | 3 | Station Assign
? | 4 | 802.11 State
? | 5 | CP User Authentication
? | 6 | 1X Authentication
? | 7 | Encryption
? | 8 | Mac Filtering

station-log> event show all
Event Filters
=====
Disp | ID# | Name
-----
? | 1 | IP Address Discovered
? | 2 | DHCP
? | 3 | Station Assign
? | 4 | 802.11 State
? | 5 | CP User Authentication
? | 6 | 1X Authentication
? | 7 | Encryption
? | 8 | Mac Filtering

station-log> event all !

```



```

station-log> event show
Event Filters
=====
Disp | ID# | Name
-----
! | 1 | IP Address Discovered
! | 2 | DHCP
! | 3 | Station Assign
! | 4 | 802.11 State
! | 5 | CP User Authentication
! | 6 | 1X Authentication
! | 7 | Encryption
! | 8 | Mac Filtering
station-log> station add 00:40:96:AA:BB:CC
Added station 00:40:96:aa:bb:cc at position 0
station-log> station show
Station Filter List
=====
Index | MAC Address
-----
0 | 00:40:96:aa:bb:cc
station-log> station del all
The station filter list has been cleared
station-log>

```

Related Commands

- [\(station-log\) filelog on page 847](#)
- [station-log show on page 855](#)

(station-log) enable

Enables station logging.

Syntax

```
station-log> enable
station-log> disable
```

Command Mode

Station Log

Default

Off

Usage

By default, station logging is disabled. Use this command to enable it.

Example

These commands enter station logging mode and turn on file logging.

```
default#configure terminal
default(config)# station-log
default(config-station-log)# enable
default(config-station-log)# end
```

Related Commands

- [station-log](#) on page 843
- [station-log show](#) on page 855

(station-log) filelog

Enables inference events logging to a system file.

Syntax

```
station-log> filelog on
station-log> filelog off
```

Command Mode

Station Log

Default

Off

Usage

If you don't want to log inference events, use this command to turn it off. The difference in performance with this logging off is not much different than performance with it on.

Example

These commands enter station logging mode and turn on file logging.

```
default#configure terminal
default(config)# station-log
default(config-station-log)# filelog on
default(config-station-log)# end
default# sh station-log-config
syslog off
filelog on
```

Related Commands

- [station-log on page 843](#)
- [\(station-log\) syslog on page 848](#)
- [station-log show on page 855](#)

(station-log) syslog

Enables logging to a system file.

Syntax

```
station-log> syslog on
station-log> syslog off
```

Command Mode

Station Log

Default

Off

Usage

If you don't want to log inference events, use this command to turn it off. The difference in performance with this logging off is not much different than performance with it on.

Example

These commands enter station logging mode and turn on file logging.

```
default#configure terminal
default(config)# station-log
default(config-station-log)# syslog on
default(config-station-log)# end
default# sh station-log-config
syslog on
filelog on
```

Related Commands

- [station-log on page 843](#)
- [\(station-log\) filelog on page 847](#)
- [station-log show on page 855](#)

(station-log) event id

Enables or disables logging for individual event types.

Syntax

```
station-log> event id show
station-log> event id set <event-id>
station-log> event id remove <event-id>
```

Command Mode

Station Log

Default

Enabled

Usage

By default, the station-log displays and logs all events listed in the example below. To view the events currently enabled, use the **event id show** command.

To enable a specific event filter, use the **event id set <id>** command, specifying the ID number desired as listed in the **event id show** command. The specified event will be filtered, and therefore will be displayed and logged as normal.

To disable a specific event filter, use the **event id remove <id>** command, specifying the ID number desired as listed in the **event id show** command. The filter will be disabled, and therefore the event information will no longer display.



To enable or disable the filter for all events, simply enter all in the id field (e.g., event id set all).

Example

```
station-log> event id show
```

Event ID Filters

=====

Enabled	ID#	Name
Yes	1	IP Address Discovered
Yes	2	DHCP
Yes	3	Station Assign

Yes		4		802.11 State
Yes		5		CP User Authentication
Yes		6		1X Authentication
Yes		7		Encryption
Yes		8		Mac Filtering
Yes		9		Diagnostics
Yes		10		Band Steering
Yes		11		SIP

Related Commands

- [station-log](#) on page 843
- [\(station-log\) filelog](#) on page 847
- [station-log show](#) on page 855

(station-log) event severity

Specifies severity levels for event types.

Syntax

```
station-log> event severity show
station-log> event severity set <event-id>
station-log> event severity remove <event-id>
```

Command Mode

Station Log

Default

Enabled

Usage

By default, the station-log displays and logs all events severity levels listed in the example below. To view the severities currently enabled, use the **event severity show** command.

To enable a specific event filter, use the **event severity set <id>** command, specifying the ID number desired as listed in the **event severity show** command. The filter will be enabled, and therefore the severity information will resume display.

To disable a specific event severity, use the **event severity remove <id>** command, specifying the ID number desired as listed in the **event severity show** command. The filter will be disabled, and therefore events of the specified severity level will no longer be displayed.



To enable or disable the filter for all events, simply enter all in the id field (e.g., event id set all).

Example

```
station-log> event severity show
```

```
Event Severity Filters
=====
Enabled | Severity
-----
Yes     | Info
Yes     | Minor
```

Yes		Major
Yes		Critical

Related Commands

- [station-log](#) on page 843
- [\(station-log\) filelog](#) on page 847
- [station-log show](#) on page 855
- [\(station-log\) event id](#) on page 849

(station-log) show filters

Displays the status of all event and severity filters in the station log.

Syntax station-log> show filters

Command Mode Station Log

Default NA

Usage To quickly view the enabled/disabled status of all station log filters, access the station-log terminal and use the command **show filters**.

Example station-log> show filters

```
Event ID Filters
=====
Enabled | ID# | Name
-----
Yes     | 1  | IP Address Discovered
Yes     | 2  | DHCP
Yes     | 3  | Station Assign
Yes     | 4  | 802.11 State
Yes     | 5  | CP User Authentication
Yes     | 6  | 1X Authentication
Yes     | 7  | Encryption
Yes     | 8  | Mac Filtering
Yes     | 9  | Diagnostics
Yes     | 10 | Band Steering
Yes     | 11 | SIP

Event Severity Filters
=====
Enabled | Severity
```

```
-----  
Yes      | Info  
Yes      | Minor  
Yes      | Major  
Yes      | Critical
```

The station filter list is empty!

Related Commands

- [station-log](#) *on page 843*
- [\(station-log\) filelog](#) *on page 847*
- [station-log show](#) *on page 855*
- [\(station-log\) event id](#) *on page 849*
- [\(station-log\) event severity](#) *on page 851*

station-log show

Lists event log history, with information such as 802.11 probe, auth, assoc, deauth, disassoc, etc. This is an alternate version of the interactive command station-log.

Syntax

```
station-log show
station-log show -mac=<station MAC address>
```

Command Mode

Global Configuration mode

Default

None

Usage

Use **station-log show** when the desired MAC address is not known and you simply want ALL of the event log history up until the current time.

Use **station-log show -mac=11:22:33:44:55:66** when you want only the history of MAC address 11:22:33:44:55:66.

Examples

This example listed all of the logged stations:

```
Master1# station-log show
2009-09-01 01:53:18.790 | 00:1c:f0:f9:02:bd | 802.11 State |
state change <old=Unauthenticated><new=Authenti-
cated><AP=00:0c:e6:05:eb:7d><BSSID=00:0c:e6:7a:29:0e>
2009-09-01 01:53:18.798 | 00:1c:f0:f9:02:bd | 802.11 State |
state change <old=Authenticated><new=Associ-
ated><AP=00:0c:e6:05:eb:7d><BSSID=00:0c:e6:7a:29:0e>
2009-09-01 01:53:18.799 | 00:1c:f0:f9:02:bd | 1X Authentication | <EAP
code=request> <EAP ID=1> <EAP type=Identity> sent
2009-09-01 01:53:19.368 | 00:20:a6:4e:c3:1b | Station Assign |
<AID=4> assigned to <AP_ID=5><ESSID=rxorn><BSSID=00:0c:e6:b1:83:0f>
2009-09-01 01:53:19.978 | 00:20:a6:4e:c3:1b | Station Assign |
<AID=4> Assign Removed From
<AP_ID=5><ESSID=rxorn><BSSID=00:0c:e6:b1:83:0f>
2009-09-01 01:53:19.978 | 00:20:a6:4e:c3:1b | Station Assign |
<AID=4> assigned to <AP_ID=4><ESSID=rxorn><BSSID=00:0c:e6:b1:83:0f>
```

```

2009-09-01 01:53:20.797 | 00:1c:f0:f9:02:bd | 1X Authentication |
<auth method=WPA2_EAP>:<pkt type=EAPOL_START> recvd <ESSID=client4>
<BSSID=00:0c:e6:7a:29:0e>

2009-09-01 01:53:20.797 | 00:1c:f0:f9:02:bd | 1X Authentication | <EAP
code=request> <EAP ID=1> <EAP type=Identity> sent

2009-09-01 01:53:21.098 | 00:16:ea:ed:c3:12 | Station Assign |
<AID=4> Assign Removed From
<AP_ID=4><ESSID=rxorn><BSSID=00:0c:e6:3d:86:0c>

2009-09-01 01:53:21.098 | 00:16:ea:ed:c3:12 | Station Assign |
<AID=1> Assign Removed From
<AP_ID=553><ESSID=rxorn><BSSID=00:0c:e6:ba:48:20>

2009-09-01 01:53:21.098 | 00:16:ea:ed:be:30 | Station Assign |
<AID=2> Assign Removed From
<AP_ID=4><ESSID=rxorn><BSSID=00:0c:e6:b1:83:0f>

2009-09-01 01:53:21.098 | 00:16:ea:ed:cf:7c | Station Assign |
<AID=6> Assign Removed From
<AP_ID=4><ESSID=rxorn><BSSID=00:0c:e6:3d:86:0c>

2009-09-01 01:53:21.174 | 00:16:ea:ed:cf:7c | Station Assign |
<AID=6> Assign Removed From
<AP_ID=4><ESSID=rxorn><BSSID=00:0c:e6:3d:86:0c>

last 2653455

```

Related Commands

- [station-log](#) on page 843
- [\(station-log\) filelog](#) on page 847
- [\(station-log\) syslog](#) on page 848

17 Service Control Commands

The commands contained in this chapter provides service control global configuration.

- [*blocked-gateway on page 858*](#)
- [*policy on page 859*](#)
- [*service-type on page 861*](#)
- [*service-control-config active-discovery on page 862*](#)
- [*service-control-config essids on page 863*](#)
- [*service-control-config gateways on page 864*](#)
- [*service-control-config locations on page 865*](#)
- [*service-control-config service-types on page 866*](#)
- [*service-control-config state on page 867*](#)
- [*service-control-config vlans on page 868*](#)
- [*show service-control blocked-gateway on page 869*](#)
- [*show service-control global-config on page 870*](#)
- [*show service-control global-config-service on page 871*](#)
- [*show service-control global-discovered-service on page 872*](#)
- [*show service-control global-discovered-service-summary on page 873*](#)
- [*show service-control location on page 874*](#)
- [*show service-control policy on page 875*](#)
- [*show service-control policy-config-service on page 876*](#)
- [*show service-control policy-service on page 877*](#)
- [*show service-control policy-service-summary on page 878*](#)
- [*show service-control service-type on page 879*](#)
- [*show service-control user-group on page 880*](#)
- [*user-group on page 881*](#)

blocked-gateway

Configure the blocked gateway using the IP address for service control.

Syntax

blocked-gateway <name>

Command Mode

Global Configuration

Default

None

Usage

Use this command to configure the IP address that is blocked for the service control.

Examples

```
controller# configure terminal
controller(config)# blocked-gateway meruip
controller(config)# exit
```

Related Commands

[show service-control blocked-gateway](#) **on page 869**

policy

Configure service control policy.

Syntax

policy

Command Mode

Global Configuration

Default

None

Usage

This command configures a unique name for the policy. You can configure role type (subscriber or publisher) user group, service types, and owner for the policy.

Examples

```
controller# configure terminal
controller(config)# policy merupolicy
MC3200(15)(config-policy)# description Fortinet Policy service control
controller(config)# exit
```

This example lists the options for the command:

```
controller# configure terminal
controller(config)# policy merupolicy
MC3200(15)(config-policy)# ?
description          (10) Specifies the Location.
end mode.            (10) Save changes, and return to privileged EXEC
exit mode.           (10) Save changes, and return to global configuration
owner                 (10) Owner of the profile
publisher-user-groups (10) Publisher User Groups.
service-types         (10) Service Types.
subscriber-user-groups (10) Subscriber User Groups.
```

Related Commands

- [show service-control policy on page 875](#)
- [show service-control policy-config-service on page 876](#)

- [*show service-control policy-service*](#) **on page 877**
- [*show service-control policy-service-summary*](#) **on page 878**
- [*show service-control service-type*](#) **on page 879**

service-type

Configure service control service type.

Syntax

service-type

Command Mode

Global Configuration

Default

None

Usage

User this command to configure the service type, its description and the service type value.

Examples

```
controller# configure terminal
controller(config)# service-type meruservicetype
MC3200(15)(config-service-type)# description Fortinet service type
controller(config)# exit
```

This example lists the options for the command:

```
controller# configure terminal
controller(config)# service-type meruservicetype
MC3200(15)(config-service-type)# ?
description          (10) Specifies the Service Type.
end
mode.                (10) Save changes, and return to privileged EXEC
exit
mode.                (10) Save changes, and return to global configuration
value                (10) Configure Value.
```

Related Commands

[show service-control service-type](#) on page 879

service-control-config active-discovery

This command triggers active-discovery per global discovery criteria.

Syntax

service-control-config active-discovery <id>/all/controller

<i>id</i>	Enter the AP ID
all	Sets all entities
controller	Sets service agent on controller

Command Mode

Global Configuration

Default

None

Usage

User this command to specify the types of services that are discovered. By default, wireless services in all SSIDs and all APs and wired services on VLAN 0 on the controller's wired interface are selected.

Examples

```
controller# configure terminal
controller(config)# service-control-config active-discovery all
controller(config)# exit
```

Related Commands

- [show service-control global-discovered-service on page 872](#)
- [show service-control global-discovered-service-summary on page 873](#)

service-control-config essids

This command adds ESSIDs to global discovery criteria.

Syntax

service-control-config essids <essids>

essids Enter comma separated ESSID profile names.

Command Mode

Global Configuration

Default

None

Usage

Use this command to discover publisher connected to this ESSID.

Examples

```
controller# configure terminal
controller(config)# service-control-config essids
controller(config)# exit
```

Related Commands

- [show service-control global-config](#) on page 870
- [show service-control global-config-service](#) on page 871

service-control-config gateways

This command configure the wired gateways for the service control.

Syntax

service-control-config gateways <gateways>

gateways Enter the AP IDs or 0 (zero) for Controller.

Command Mode

Global Configuration

Default

None

Usage

Use this command to add APs and/or Controllers to wired gateway list for discovery of publisher.

Examples

```
controller# configure terminal  
controller(config)# service-control-config gateways  
controller(config)# exit
```

Related Commands

[show service-control blocked-gateway](#) *on page 869*

service-control-config locations

This command configures the locations for service control.

Syntax

service-control-config locations <location name>

location Enter the location name to activate the service control.

Command Mode

Global Configuration

Default

None

Usage

Use this command to specify locations for wireless subscriber/publisher.

Examples

```
controller# configure terminal
controller(config)# service-control-config locations
controller(config)# exit
```

Related Commands

[show service-control location](#) on page 874

service-control-config service-types

This command configures the service types.

Syntax

service-control-config service-types <service types>

service-types Enter the service types that would be available in the network.

Command Mode

Global Configuration

Default

None

Usage

Use this command to configure the available service and its service types.

Examples

```
controller# configure terminal
controller(config)# service-control-config service-types AppleTV
controller(config)# exit
```

Related Commands

- [show service-control policy-service on page 877](#)
- [show service-control policy-service-summary on page 878](#)
- [show service-control service-type on page 879](#)

service-control-config state

This command enable or disables the service control.

Syntax

service-control-config state <enable/disable>

<i>enable</i>	Enables the service control feature in the network
<i>disable</i>	Disables the service control feature in the network.

Command Mode

Global Configuration

Default

None

Usage

Examples

```
controller# configure terminal
controller(config)# service-control-config state enable
controller(config)# exit
```

Related Commands

[show service-control global-config](#) on page 870

service-control-config vlans

This command configures VLAN in global discovery criteria for wired gateway.

Syntax

service-control-config vlan <vlans>

vlans Enter comma-separated and range of VLAN IDs.

Command Mode

Global Configuration

Default

None

Usage

Examples

```
controller# configure terminal
controller(config)# service-control-config vlan 10
controller(config)# exit
```

Related Commands

[show service-control global-config](#) on page 870

show service-control blocked-gateway

Displays blocked gateways list.

Syntax `show service-control blocked-gateway`

Command Mode User EXEC

Default None

Usage This command displays the list of blocked IP address from which advertisement are ignored.

Examples

```
controller# show service-control blocked-gateway
Name           IP Address
Fortinet       172.29.0.137
               Servcie Connect Blocked Gateway(1 entry)
```

Related Commands

- [blocked-gateway](#) on page 858
- [service-control-config gateways](#) on page 864

show service-control global-config

Displays configured global discovery criteria.

Syntax `show service-control global-config`

Command Mode User EXEC

Default None

Usage The command displays the global configuration for service control including the service type list, VLANs, ESSID profile, location list, and wired gateway list.

Examples controller# `show service-control global-config`
service control Global Configuration

```
Enable Service      : enable
Service Type List   : *
VLANs               : 0
ESSIDs              : Dabcjk
Location List       : MeruEng
Wired Gateway List  : 0
```

- Related Commands**
- [service-control-config active-discovery](#) on page 862
 - [service-control-config essids](#) on page 863
 - [service-control-config gateways](#) on page 864
 - [show service-control global-config-service](#) on page 871

show service-control global-config-service

Displays configured global discovery criteria of services.

Syntax `show service-control global-config-service`

Command Mode User EXEC

Default None

Usage This command lists the service control global configuration services that are available.

Examples `controller# show service-control global-config-service`

Related Commands

- [service-control-config essids](#) *on page 863*
- [service-control-config gateways](#) *on page 864*
- [show service-control global-config](#) *on page 870*

show service-control global-discovered-service

Displays global discovered service list.

Syntax `show service-control global-discovered-service`

Command Mode User EXEC

Default None

Usage

Examples `controller# show service-control global-discovered-service`

Related Commands

- [service-control-config active-discovery](#) **on page 862**
- [show service-control global-discovered-service-summary](#) **on page 873**

show service-control global-discovered-service-summary

Displays global discovered service summary.

Syntax `show service-control global-discovered-service-summary`

Command Mode User EXEC

Default None

Usage This command lists the summary of the types of services that are discovered.

Examples `controller# show service-control global-discovered-service-summary`

Related Commands

- [service-control-config active-discovery](#) on page 862
- [show service-control global-discovered-service](#) on page 872

show service-control location

Displays service control locations.

Syntax `show service-control location`

Command Mode User EXEC

Default None

Usage

Examples

```
controller# show service-control location
```

Name	AP ID	Description
FortiEng	10,6-9	Fortinet Engineering Area
FortiTest	1-5	Fortinet Test

Location(2)

Related Commands [service-control-config locations](#) on page 865

show service-control policy

Displays service control policies.

Syntax `show service-control policy`

Command Mode User EXEC

Default None

Usage

Examples

```
controller# show service-control policy
Name          Subscriber User Group   Service Type   Publisher User Group
MeruPolicy    MeruUSER                *              MeruUSER
               service control Policy(1 entry)
```

- Related Commands**
- [policy on page 859](#)
 - [show service-control policy-config-service on page 876](#)
 - [show service-control policy-service on page 877](#)
 - [show service-control policy-service-summary on page 878](#)

show service-control policy-config-service

Displays policies and its configuration.

Syntax `show service-control policy-config-service`

Command Mode User EXEC

Default None

Usage

Examples

```
controller# show service-control policy-config-service
```

Policy	Service Type	List	Sub APs	Sub VLANs	Sub ESSIDs
Sub Cont	Pub APs	Pub VLANs	Pub ESSIDs	Pub Cont	
1	_airplay._tcp.local.,_r	6-10			1
enable	6-10		1		enable

Policy Configuration Service(1 entry)

- Related Commands**
- [policy on page 859](#)
 - [show service-control policy on page 875](#)
 - [show service-control policy-service on page 877](#)
 - [show service-control policy-service-summary on page 878](#)

show service-control policy-service

Displays filtered list of services and its service type available to the subscriber.

Syntax

`show service-control policy-service <name>`

Command Mode

User EXEC

Default

None

Usage

Examples

controller# `show service-control policy-service merupolicysrv`

Related Commands

- [*policy on page 859*](#)
- [*show service-control policy on page 875*](#)
- [*show service-control policy-config-service on page 876*](#)
- [*show service-control policy-service-summary on page 878*](#)

show service-control policy-service-summary

Displays summary list of services.

Syntax `show service-control policy-config-service-summary <name>`

Command Mode User EXEC

Default None

Usage This command provides a summary of the policy service configured.

Examples `controller# show service-control policy-service-summary merupolicy`

Related Commands

- [*policy on page 859*](#)
- [*show service-control policy on page 875*](#)
- [*show service-control policy-config-service on page 876*](#)
- [*show service-control policy-service on page 877*](#)

show service-control service-type

Displays list of service types.

Syntax `show service-control service-type`

Command Mode User EXEC

Default None

Usage

Examples

```
controller# show service-control service-type
Name           Description    Service Type
AppleTV        Apple TV      _airplay._tcp.local.,_raop._tcp.local.
Printer        Printer       _ipp._tcp.local.,_ipps._tcp.local.,_uni
Service Type(2)
```

Related Commands [service-type](#) on page 861

show service-control user-group

Displays service control user groups.

Syntax `show service-control user-group`

Command Mode User EXEC

Default None

Usage

Examples

```
controller# show service-control user-group
Name          VLAN          ESSIDs      Locations
MeruUSER      100            Dabcjk      MeruEng
               User Group(1 entry)
```

Related Commands [user-group](#) on page 881

user-group

Configure service control user group

Syntax

user-group

Command Mode

Global Configuration

Default

None

Usage

This command configures a unique name for the user group. You can configure role type (subscriber or publisher), ESSID list, locations, and VLAN list for the user group.

Examples

```
controller# configure terminal
controller(config)# user-group
MC3200(15)(config-user-group)# description Fortinet User Group
MC3200(15)(config-user-group)# enable-pub-role on
controller(config)# exit
```

This example lists the options for the command:

```
controller# configure terminal
controller(config)# user-group
MC3200(15)(config-user-group)# ?
description          (10) Specifies the User Group.
enable-pub-role      (10) Configure Publisher Role.
enable-sub-role      (10) Configure Subscriber Role.
end                  (10) Save changes, and return to privileged EXEC mode
essids                (10) Configure ESSID list.
exit                 (10) Save changes, and return to global configuration
mode.
locations            (10) Configure Location list.
vlans                (10) Configure VLAN list.
```

Related Commands

show service-control user-group **on page 880**

18 Troubleshooting Commands

The commands that help troubleshoot the WLAN are:

- [*analyze-capture*](#) **on page 885**
- [*auto-report admin*](#) **on page 886**
- [*auto-report send*](#) **on page 888**
- [*capture-packets*](#) **on page 890**
- [*debug captive-portal*](#) **on page 897**
- [*debug connect*](#) **on page 898**
- [*debug controller*](#) **on page 899**
- [*debug eap*](#) **on page 900**
- [*debug mac-filter*](#) **on page 901**
- [*debug module*](#) **on page 902**
- [*\(diag-log\) admin*](#) **on page 906**
- [*\(diag-log\) config*](#) **on page 908**
- [*\(diag-log\) restore*](#) **on page 910**
- [*diagnostics*](#) **on page 912**
- [*diagnostics-ap*](#) **on page 914**
- [*diagnostics-controller*](#) **on page 916**
- [*\(packet-capture-profile\) enable-profile*](#) **on page 930**
- [*\(packet capture profile\) mode*](#) **on page 934**
- [*packet-capture-profile*](#) **on page 918**
- [*\(packet capture profile\) ap-list*](#) **on page 921**
- [*\(packet capture profile\) capture-sibling-frames*](#) **on page 923**
- [*\(packet-capture-profile\) enable-profile*](#) **on page 930**
- [*\(packet capture profile\) filter*](#) **on page 932**
- [*\(packet capture profile\) interface list*](#) **on page 933**
- [*\(packet capture profile\) mode*](#) **on page 934**

- [\(packet capture profile\) packet-truncation-length](#) on page 936
- [\(packet capture profile\) rate-limiting](#) on page 937
- [\(packet capture profile\) rate-limiting-mode](#) on page 939
- [\(packet capture profile\) rtx](#) on page 940
- [\(packet capture profile\) token-bucket-rate](#) on page 942
- [\(packet capture profile\) token-bucket-size](#) on page 945
- [remote-log](#) on page 948
- [show auto-report-config](#) on page 949
- [show cef](#) on page 951
- [show debug](#) on page 952
- [show diag-log-config ap/controller/station](#) on page 953
- [show packet-capture-profile](#) on page 959
- [show statistics AP300-diagnostics](#) on page 961

analyze-capture

Analyzes wireless traffic.

Syntax

```
analyze-capture snapshot  
analyze-capture start <filename> ap <ap-list> bssid <bssid-list>  
analyze-capture stop
```

Command Mode

Privileged EXEC

Default

None

Usage

The **analyze-capture** command captures 802.11 management and TCP session state statistics for all clients using any of the specified APs and BSSIDs. The type of information that is collected are client re-auths and re-associations and TCP session statistics.

The command can be started and run for long periods without consuming disk space. No output is produced until the **snapshot** or **stop** keywords are given.

Double quotes must be used to group a string of APs or BSSIDs.

Examples

As an example, the following command creates the capture in file `check.txt` for APs 1-3 and BSSIDs 00:0c:e6:32:22:01 and 00:0c:e6:30:11:22.

```
controller# analyze-capture start check.txt ap "1 2 3" bssid  
"00:0c:e6:32:22:01 00:0c:e6:30:11:22"  
controller#
```

Related Commands

[packet-capture-profile](#) on page 918

auto-report admin

Use this command only when you are working with Fortinet support. This command turns auto-reporting on and off so that you can send diagnostic information to Fortinet Support.

Syntax

```
auto-report admin on
auto-report admin off
```

Command Mode

Configuration mode

Default

off

Usage

This command works with the command **auto-report send**. If you specify an interval in **auto-report send**, the report will be sent on that schedule as long as **auto-report admin** is set to **on**.

Example

This example sends a report to `cwon:cwon@172.27.0.79/diagagent.conf` every hour:

```
default#configure terminal
default(config)# auto-report
default(config-auto-report)# ?
```

```
admin    Configures administration mode for auto-reporting
do       Executes an IOSCLI command
end      Saves changes and returns to privileged exec mode
exit     Saves changes and returns to global configuration mode
send     Uploads log files to named URL once or periodically
```

```
default(config-auto-report)# send ftp://cwon:cwon@172.27.0.79/diag-
gent.conf 1
default(config-auto-report)# admin on
default(config-auto-report)# show auto-report-config
```

```
Administration Status      on
Auto-reporting Interval    every hour
Auto-reporting URL         cwon:cwon@172.27.0.79
```

Related Commands

- [auto-report send](#) on page 888
- [\(diag-log\) admin](#) on page 906
- [\(diag-log\) config](#) on page 908
- [\(diag-log\) restore](#) on page 910
- [show auto-report-config](#) on page 949

auto-report send

Use this feature only when working with Customer Support. This command converts the information in diagnostic log files to an encrypted report, sends the report using FTP, and then clears the log file.

Syntax

`auto report send <username:password> <URL Location><interval>`

<i>username</i>	FTP user name - required.
<i>password</i>	FTP password - required.
<i>URL location</i>	IP address for the upload
<i>interval</i>	How often to send the report in hours. 24 would be once a day.

Command Mode

Global Configuration

Default

none

Usage

This command converts the information in diagnostic log files to an encrypted report, sends the report, and then clears the log file. If you specify an interval, the report will be sent on that schedule as long as **auto-report admin** is set to **on**. You must use a password in the URL. If there is no login name, use anonymous and the password anonymous. If the password field is empty you will not be able to untar the file.

Example

This example sends a report to anonymous:anonymous@192.168.105.75 1 every hour:

```
default#configure terminal
default(config)# auto-report
default(config-auto-report)# ?
```

<code>admin</code>	Configures administration mode for auto-reporting
<code>do</code>	Executes an IOSCLI command
<code>end</code>	Saves changes and returns to privileged exec mode
<code>exit</code>	Saves changes and returns to global configuration mode
<code>send</code>	Uploads log files to named URL once or periodically

```
default(config-auto-report)# send ftp://anonymous:anonymous@192.168.105.75
1
default# sh auto-report-config
Administration Status on
Auto-Reporting Interval every 1 hour
Auto-Reporting Url ftp://anonymous:anonymous@192.168.105.75
Administration Status          on
Auto-reporting Interval        every hour
Auto-reporting URL             cwon:cwon@172.27.0.79
```

Related Commands

- [auto-report admin](#) on page 886
- [\(diag-log\) admin](#) on page 906
- [\(diag-log\) config](#) on page 908
- [\(diag-log\) restore](#) on page 910
- [show auto-report-config](#) on page 949

capture-packets

Use this command for AP150 packet capture. For AP300 and AP200, you can use the newer, more robust FortiWLC (SD) commands in [packet-capture-profile](#) on [page 918](#) mode. The **capture-packets** command is still supported and any scripts that use the command will still run exactly the same way as they did with previous releases and is the only option for AP150.

Captures packets, using Ethereal, on the controller's interface or over the air from access points.

Syntax

```
capture-packets [-c count][-i ap_id1[, ap_id2, ...]] {m,n,t}[-r infile] [-R filter]r|a|ad|d [-V] [-v frame] [-w savefile -a stop-condition] [-x]
```

-a <i>stop-condition</i>	Stop criterion (e.g. -a filesize:1000)
-c <i>count</i>	Specifies the default number of packets to read when capturing live data.
-f <i>capture-filter</i>	Filter expression
-F <i>file-format</i>	Format of the capture file (for example, -F netmon1).
-i <i>ap_id1[, ap_id2, ...]</i>	Captures packets from an AP (specified by its number), followed by optionally, a list of additional APs.
-n	Disables network object name resolution (such as host-name, TCP, and UDP port names).
-N { <i>m,n,t</i> }	Enables name resolution for particular types of addresses and port numbers, with name resolving for other types of addresses and port numbers turned off. The argument is a string that can contain the letters m to enable MAC address resolution, n to enable network address resolution, and t to enable transport-layer port number resolution. This argument overrides the -n argument if both -N and -n are present.
-p	Disables promiscuous mode for the interface.
-q	Do not display count of packets captured.
-r <i>infile</i>	Prints a summary of a previously captured file with an additional field (frame number) in the first column.

-R <i>'display-filter'</i>	Applies a custom or Ethereal filter before displaying captures. Build complex filters by enclosing filter names between single quotation marks (") and joining with expression operators. Do not use spaces with complex filters, that is, those that use operators such as ==. See the table that follows for a list of custom filters you can use with this argument. For information about Ethereal filters, see http://www.ethereal.com/docs/man-pages/ethereal-filter.4.html .
-S <i>Record</i>	Record/summarize with frame number for playback.
-s <i>snaplen</i>	<i>snaplen</i> defines the default snapshot length of live data.
-t <i>r a ad d</i>	Defines the format of the packet timestamp displayed in the packet list window. The format can be one of r (relative), a (absolute), ad (absolute with date), or d (delta). The relative time is the time elapsed between the first packet and the current packet. The absolute time is the actual time the packet was captured, with no date displayed; the absolute with date is the time the packet was captured. The delta time is the time since the previous packet was captured. The default is relative.
-V	Prints the protocol tree.
-v <i>frame</i>	Play back with frame number.
-w <i>savefile</i> -a <i>stop-condition</i>	Writes capture information to a file and limits the file size. Fortinet recommends that you use the -w and -a arguments together, using filesize:5000 as the <i>stop-condition</i> parameter, which limits the file size to 5 MB.
-x	Displays packet capture in hexadecimal format.
-S <i>record</i>	Record/summarize with frame number for playback
-v <i>playback</i>	Frame playback "frame number"

Command Mode

Global configuration

Default

None

Usage

Use the **capture-packets** command to capture AP150 network traffic. Use the **capture-packets** command with no arguments to capture packets on the controller's interface. The **capture-packets** command can also capture packets from access points if you issue the **debug ap** command first. You can filter the packets so that you only see packets captured by

access points. By default, you see packets from access points and the controller's local interface. You can see the captures in realtime or save them to a file for future offline analysis. If you are using SSH to access the controller, consider filtering SSH traffic to reduce the amount of information that gets captured and displayed. (See "Examples" on page 626 for an example.) Use **capture-packets** on AP150 only when the interface filter or MAC address filters are set. Without these filters set, the AP150 gets overwhelmed with the amount of data and eventually loses contact with the controller.

To stop realtime packet capture, press **Ctrl-C**.

Packets captured by the access point include traffic from unknown access points and traffic between access points. Use the **-R** argument to filter the packets captured. (See the following table for a list of custom filters.)

WEP-encrypted frames are encrypted when captured over the air. To capture unencrypted data frames, get captures from the controller's local interface. If you use static WEP keys, frames can be decoded using the Windows version of Ethereal with the Fortinet plug-in.

Packets transmitted by an access point are different from packets received by an access point in the following ways:

- There is one packet for every retry received by the access point. The retry bit is set as received over the air. Transmitted frames only appear once, regardless of the number of retransmissions. Use the controller.cap.tx.flags.retries field to see the number of times a frame was retried. The retry bit of the 802.11 MAC header is always set to zero for transmitted frames.
- For received frames, the TSF field is the exact time the first bit a frame was received. For transmitted frames, the TSF field is the time immediately after the last transmission.
- Received 802.11 acknowledgments are captured, but transmitted acknowledgments are not.

Captured frames that exceed the Ethernet MTU are fragmented. When looking at capture entries, the second entry for a fragmented frame appears as "M-Cap 802.11 Continuation Controller ATS Capture Fragment Continuation" as the summary.

The following lists the filters that can be used with the **-R** argument for the **capture-packets** command:

controller.cap	Limits only packets captured by the access point and excludes packets from the controller's local interface.
controller.cap.version	Version of the tunnel.

controller.cap.outer.fraglen	Length of the fragment
controller.cap.frag	Fragment field
controller.cap.outer.fragmented	Fragmented
controller.cap.outer.morefrags	More fragments
controller.cap.outer.fragnumber	Fragment number
controller.cap.outer.seq	Direction of captured frame (transmitted or received)
controller.cap.rx.flags	Receive flags
controller.cap.rx.flags.diversity	Received with antenna diversity
controller.cap.rx.flags.antenna_select	Antenna frame received on
controller.cap.rx.flags.shortpreamble	Short preamble
controller.cap.rx.flags.assigned	Whether the sender is assigned to this AP
controller.cap.rx.flags.fcs_failure	Whether the checksum is valid
controller.cap.rx.flags.frame_too_late	Whether a frame was received too late from carrier sense to make sense
controller.cap.rx.silence	Signal strength immediately before the packet.
controller.cap.rx.signal	Signal strength during the packet.
controller.cap.rx.left_rssi	RSSI from the left antenna.
controller.cap.rx.right_rssi	RSSI from the right antenna.
controller.cap.rx.rate	802.11 packet rate (in 100 Kbps).
controller.cap.rx.cca_dclk	Time from the CCA high to the first data bit (in microseconds)
controller.cap.rx.length	Length of the received 802.11 frame
controller.cap.rx.time	Lower TSF time the frame
controller.cap.rx.channel	Channel the frame was received on
controller.cap.rx.crc	802.11 FCS
controller.cap.tx.flags	Transmit flags
controller.cap.tx.flags.success	Whether an 802.11 acknowledgement was received
controller.cap.tx.flags.initcts	If an RTS was sent for the initial transmission, indicates whether a CTS was received
controller.cap.tx.flags.retry1cts	If an RTS was sent for the first retransmission, indicates whether a CTS was received

controller.cap.tx.flags.retry2cts	If an RTS was sent for the second retransmission, indicates whether a CTS was received
controller.cap.tx.flags.retry3cts	If an RTS was sent for the third retransmission, indicates whether a CTS was received
controller.cap.tx.flags.retry4cts	If an RTS was sent for the fourth retransmission, indicates whether a CTS was received
controller.cap.tx.flags.retry5cts	If an RTS was sent for the fifth retransmission, indicates whether a CTS was received
controller.cap.tx.flags.retry6cts	If an RTS was sent for the sixth retransmission, indicates whether a CTS was received
controller.cap.tx.flags.retry7cts	If an RTS was sent for the seventh retransmission, indicates whether a CTS was received
controller.cap.tx.flags.ackps	PS bit of acknowledgment (if any)
controller.cap.tx.flags.ackrssi	RSSI of acknowledgment (if any)
controller.cap.tx.flags.retries	Retransmissions attempted (zero if frame transmitted only once)
controller.cap.tx.flags.antenna	Antenna frame transmitted on
controller.cap.tx.flags.preamble	Short preamble used to transmit the frame (or final frame if retried)
controller.cap.tx.time	Lower TSF time the frame was transmitted (or final frame if retried)
controller.cap.tx.length	Length of the 802.11 frame
controller.cap.tx.rate	Rate used to transmit the frame (or final frame if retried)
controller.cap.tx.channel	Channel the frame was transmitted on

Examples

The following command captures only ICMP packets:

```
controller# capture-packets -R icmp
Capturing on controller
30.434804 10.1.225.50 -> 10.1.250.15 ICMP Echo (ping) request
30.435000 10.1.250.15 -> 10.1.225.50 ICMP Echo (ping) reply
31.433751 10.1.225.50 -> 10.1.250.15 ICMP Echo (ping) request
31.433866 10.1.250.15 -> 10.1.225.50 ICMP Echo (ping) reply
32.432920 10.1.225.50 -> 10.1.250.15 ICMP Echo (ping) request
32.433042 10.1.250.15 -> 10.1.225.50 ICMP Echo (ping) reply
```

```

33.432088 10.1.225.50 -> 10.1.250.15 ICMP Echo (ping) request
33.432203 10.1.250.15 -> 10.1.225.50 ICMP Echo (ping) reply
34.431320 10.1.225.50 -> 10.1.250.15 ICMP Echo (ping) request
34.431434 10.1.250.15 -> 10.1.225.50 ICMP Echo (ping) reply
35.430419 10.1.225.50 -> 10.1.250.15 ICMP Echo (ping) request
35.430523 10.1.250.15 -> 10.1.225.50 ICMP Echo (ping) reply
36.429761 10.1.225.50 -> 10.1.250.15 ICMP Echo (ping) request
36.429860 10.1.250.15 -> 10.1.225.50 ICMP Echo (ping) reply

```

The following command filters SSH traffic:

```
controller# capture-packets -R 'tcp.srcport!=22&&tcp.dstport!=22'
```

The following command captures packets to a file named **capture-file** with a maximum file size of 5 MB:

```
controller# capture-packets -w capture-file -a filesize:5000
```

Capturing on controller

559

```
controller#
```

The following command captures only RADIUS frames to and from the IP address 10.1.225.42:

```
controller# capture-packets -w capture_file -a filesize:5000 -R
'ip.addr==10.1.225.42&&radius'
```

The following commands filter for DHCP frames, which are saved to a file named capture_file, and show the captured file:

```
controller# debug ap 1
```

```
controller# capture-packets -w capture_file -a filesize:5000 -R bootp.dhcp
```

```
controller# capture-packets -r capture_file
```

```

  1  0.000000 10.0.220.49 -> 10.0.0.10  DHCP DHCP Request  - Transaction
      ID 0x9a5e380e
  2  0.002390 10.0.0.10 -> 10.0.220.49  DHCP DHCP ACK      - Transaction
      ID 0x9a5e380e

```

The following commands filter for all traffic on BSS 00:0c:e6:01:00:0d, all traffic to and from client 00:07:40:01:02:03, and all EAPOL traffic, respectively:

```
controller# capture-packets -R 'wlan.bssid==00:0c:e6:01:00:0d'  
controller# capture-packets -R 'wlan.addr==00:07:40:01:02:03'  
controller# capture-packets -R eapol
```

Related Commands

[packet-capture-profile](#) *on page 918*

debug captive-portal

Enable debug messages for Captive Portal.

Syntax

```
debug captive portal  
no debug captive portal
```

Command Mode

Privileged EXEC

Default

None

Usage

Use this debugging module to validate Captive Portal authentication. This debug information provides details about the end to end packet transfer between the wireless supplicant and the authentication server. Note that you can have multiple Captive Portal login pages, but there is only one Captive Portal.

Examples

The following example turns Captive Portal debugging on and then off.

```
demo# debug captive-portal  
OK!  
demo# no debug captive-portal  
demo#
```

Related Commands

[captive-portal](#) on page 388

debug connect

Enable debug messages for 802.11 connection.

Syntax

```
debug connect  
no debug all
```

Command Mode

Privileged EXEC

Default

None

Usage

This debugging module provides information about the 802.11 process performed from a wireless client, specifically 802.11 Probe, Auth, Assoc, Deauth, Disassoc etc. We recommend that you use the newer [station-log on page 843](#) command for this debugging rather than this command.

Examples

The following example turns on debugging for the 802.11 connection:

```
demo# debug connect  
OK!  
demo# no debug connect
```

Related Commands

[station-log on page 843](#)

debug controller

Enables real-time tracing on the controller.

Syntax

```
debug controller
no debug controller
```

Command Mode

Privileged EXEC

Default

None

Usage

After specifying a trace facility using the **debug module** command, use the **debug controller** command to enable tracing on the controller. All trace information is shown on the controller console window.

To disable tracing, use the **no** form. The **no** form disables all debug module commands previously entered.

Examples

The following command enables tracing on the controller and shows an abbreviated debug message list:

```
controller# debug controller
```

```
Real-time trace display enabled for severity >= 0.
```

```
controller# [08/05 14:29:06.190] QOS: RsrcTopoMsgProcessor: topo-rm msg
type = 0, len= 52.
```

```
[08/05 14:29:24.230] QOS: RsrcTopoMsgProcessor: topo-rm msg type = 0, len=
52.
```

```
[08/05 14:29:27.047] SEC: ieee802_1x_receive: Set NAS-port to <2051>
```

```
[08/05 14:29:27.048] SEC: Received EAPOL-START frame from client
(00:0e:35:09:5d:5e).
```

```
[08/05 14:29:27.048] SEC: Sending EAPOL-EAP Request-Identity to client
(00:0e:35:09:5d:5e), ID (1).
```

Related Commands

[debug module](#) on page 902

debug eap

Enable the display of debug messages for Extensible Authentication Protocol.

Syntax

```
debug eap
no debug all
```

Command Mode

Privileged EXEC

Default

None

Usage

Extensible Authentication Protocol is an authentication framework, not a specific authentication mechanism. The EAP provides some common functions and a negotiation of the desired authentication mechanism. Such mechanisms are called EAP methods and there are currently about 40 different methods. When EAP is invoked by an 802.1X enabled NAS (Network Access Server) device such as an 802.11 a/b/g Wireless Access Point, EAP methods can provide a secure authentication mechanism and negotiate a secure PMK (Pair-wise Master Key) between the client and NAS. The PMK can then be used for the wireless encryption session which uses TKIP or CCMP (based on AES) encryption.

Examples

The following example turns EAP debugging on and then off.

```
demo# debug eap
OK!
# no debug all
```

Related Commands

debug mac-filter

Enable the display of debug messages for MAC filtering.

Syntax

```
debug mac filter
no debug all
```

Command Mode

Privileged EXEC

Default

None

Usage

Examples

The following example turns MAC filter debugging on and then off.

```
demo# debug mac-filter
OK!
demo# no debug all
```

Related Commands

[macfiltering](#) on page 436

debug module

Enables tracing for a specific facility.

Syntax

```
debug module ip
debug module coord
debug modulesec
no debug module
```

ip	Specifies DHCP trace facility.
coord	Specifies client-access point assignment trace facility.
sec	Specifies security trace facility.

Command Mode

Privileged EXEC

Default

None

Usage

Use the **debug module** command to specify a trace. You can issue the **debug module** command multiple times with different keywords. After specifying a facility to trace, enable tracing on the controller with the **debug controller** command to send trace information to the controller console. After issuing the command **debug module coord**, you must specify the parameter for the mask. Therefore, the commands will be **debug module <xxx> mask <hex value>**.

Examples

The following commands specify security and DHCP as the facilities to trace:

```
demo# debug module sec
OK!
demo# debug controller
Real-time trace display enabled for severity >= 0.
demo# [04/13 20:21:19.201] HANDOFF: CleanupTopo: Cleaning up STAs and edges
[04/13 20:21:19.201] HANDOFF: CleanupTopo: ESS [3dot7wpa2psk] BSSID
[00:0c:e6:00:01:40] CUR STA <0/0> vs MAX <0>, channel 44, interface 2
[04/13 20:21:19.201] HANDOFF: CleanupTopo: ESS [3dot7wpa2psk] BSSID
[00:0c:e6:00:01:40] CUR STA <0/0> vs MAX <0>, channel 44, interface 2
```

```

[04/13 20:21:25.211] HANDOFF: CleanupTopo: Cleaning up STAs and edges
[04/13 20:21:25.211] HANDOFF: CleanupTopo: ESS [3dot7wpa2psk] BSSID
[00:0c:e6:00:01:40] CUR STA <0/0> vs MAX <0>, channel 44, interface 2
[04/13 20:21:25.211] HANDOFF: CleanupTopo: ESS [3dot7wpa2psk] BSSID
[00:0c:e6:00:01:40] CUR STA <0/0> vs MAX <0>, channel 44, interface 2
[04/13 20:21:31.231] HANDOFF: CleanupTopo: Cleaning up STAs and edges
[04/13 20:21:31.231] HANDOFF: CleanupTopo: ESS [3dot7wpa2psk] BSSID
[00:0c:e6:00:01:40] CUR STA <0/0> vs MAX <0>, channel 44, interface 2
[04/13 20:21:31.231] HANDOFF: CleanupTopo: ESS [3dot7wpa2psk] BSSID
[00:0c:e6:00:01:40] CUR STA <0/0> vs MAX <0>, channel 44, interface 2
[04/13 20:21:37.242] HANDOFF: CleanupTopo: Cleaning up STAs and edges
[04/13 20:21:37.242] HANDOFF: CleanupTopo: ESS [3dot7wpa2psk] BSSID
[00:0c:e6:00:01:40] CUR STA <0/0> vs MAX <0>, channel 44, interface 2
[04/13 20:21:37.242] HANDOFF: CleanupTopo: ESS [3dot7wpa2psk] BSSID
[00:0c:e6:00:01:40] CUR STA <0/0> vs MAX <0>, channel 44, interface 2
[04/13 20:21:43.261] HANDOFF: CleanupTopo: Cleaning up STAs and edges
[04/13 20:21:43.262] HANDOFF: CleanupTopo: ESS [3dot7wpa2psk] BSSID
[00:0c:e6:00:01:40] CUR STA <0/0> vs MAX <0>, channel 44, interface 2
demo# no debug controller
OK!
demo# no debug module sec
OK!
demo# debug module ip
OK!
demo# no debug module ip
OK!
demo#

```

This command specifies the client-access point assignment trace facility:

```

default# sup-cli
default] tr coord
On? FlagValue Description
-----
00000001 Assign Manager
00000002 Beacon Manager
00000004 Configuration
00000008 Dispatcher
00000010 Handoff Manager
00000020 InterCell Manager

```

```

00000040 Main Thread
00000080 Nms Agent
00000100 Resource Manager
00000200 Time Estimator
00000400 Timer Scheduler
00000800 Topology Graph
00001000 Topology Manager
00004000 Memory Usage
00008000 Message Stats
00010000 Assign Manager Detail
00020000 Beacon Manager Detail
00040000 Configuration Detail
00080000 Dispatcher Detail
00100000 Handoff Manager Detail
00200000 InterCell Manager Detail
00400000 Main Thread Detail
00800000 Nms Agent Detail
01000000 Resource Manager Detail
02000000 Time Estimator Detail
04000000 Timer Scheduler Detail
08000000 Topology Graph Detail
10000000 Topology Manager Detail
20000000 General
40000000 Test
80000000 Customer
-----
00000000 = Current Mask
default]
default] exit
default# debug module coord mask 0000FFFF
OK!
default# sup-cli
default] tr coord
On? FlagValue Description
-----
* 00000001 Assign Manager
* 00000002 Beacon Manager

```

```

* 00000004 Configuration
* 00000008 Dispatcher
* 00000010 Handoff Manager
* 00000020 InterCell Manager
* 00000040 Main Thread
* 00000080 Nms Agent
* 00000100 Resource Manager
* 00000200 Time Estimator
* 00000400 Timer Scheduler
* 00000800 Topology Graph
* 00001000 Topology Manager
* 00004000 Memory Usage
* 00008000 Message Stats
00010000 Assign Manager Detail
00020000 Beacon Manager Detail
00040000 Configuration Detail
00080000 Dispatcher Detail
00100000 Handoff Manager Detail
00200000 InterCell Manager Detail
00400000 Main Thread Detail
00800000 Nms Agent Detail
01000000 Resource Manager Detail
02000000 Time Estimator Detail
04000000 Timer Scheduler Detail
08000000 Topology Graph Detail
10000000 Topology Manager Detail
20000000 General
40000000 Test
80000000 Customer
-----
0000ffff = Current Mask
default]

```

Related Commands

debug controller on page 899

(diag-log) admin

Use this feature only when working with Customer Support. Turns diagnostics administration status on and off for the controller, AP, or station.

Syntax

```
admin station on
admin controller on
admin ap on
admin station on
admin station off
admin controller off
admin ap off
```

Command Mode

configure terminal > diag-log

Default

None

Usage

Once you turn on Diagnostic Inferences, you can see the results with the Web UI interface at **Monitor > Diagnostics > Inferences** or with the CLI command **show station counter**.

Example

These commands turn on diagnostic Inferences.

```
default# configure terminal
default(config)# diag-log
default(config-diag-log)# admin controller on
default(config-diag-log)# admin ap on
default(config-diag-log)# admin station on
```

This example lists the options for the command:

```
corpwifi# configure terminal
corpwifi(config)# diag-log
corpwifi(config-diag-log)# ?
admin                Manages diagnostics admin status.
config               Download diagnostics configuration file from url.
do                   Executes an IOSCLI command.
end                  Save changes, and return to privileged EXEC mode.
```

exit	Save changes, and return to global configuration
mode.	
restore	Restores to default diagnostics configuration file.

```
corpwifi(config-diag-log)# admin ?
ap                Configure admin mode for AP diagnostics.
controller        Configure admin mode for controller diagnostics.
station           Configure admin mode for station diagnostics.
corpwifi(config-diag-log)# admin ap ?
off               Turn off AP diagnostics.
on                Turn on AP diagnostics.
corpwifi(config-diag-log)# exit
```

Related Commands

- [auto-report admin](#) on page 886
- [auto-report send](#) on page 888
- [\(diag-log\) config](#) on page 908
- [\(diag-log\) restore](#) on page 910
- [show auto-report-config](#) on page 949

(diag-log) config

Use this feature only when working with Customer Support. Downloads diagnostics configuration file from a URL.

Syntax

`config <url>`

Command Mode

`configure terminal > diag-log`

Default

none

Usage

Diagnostics configuration changes can only be done by Fortinet support. If Fortinet support altered a diagnostics configuration file for you, you can implement it with the command **config**. Note that you can return to the default configuration with the command [\(diag-log\) restore on page 910](#).

Examples

This example downloads a configuration file from the location `cwon:cwon@182.27.0.79`:

```
default# configure terminal
default(config)# diag-log
default(config-diag-log)# config cwon:cwon@182.27.0.79
```

This example lists the options for the command:

```
corpwifi# configure terminal
corpwifi(config)# diag-log
corpwifi(config-diag-log)# ?
admin                Manages diagnostics admin status.
config               Download diagnostics configuration file from url.
do                   Executes an IOSCLI command.
end                  Save changes, and return to privileged EXEC mode.
exit                 Save changes, and return to global configuration
mode.
restore              Restores to default diagnostics configuration file.
corpwifi(config-diag-log)# config ?
```


<url> The url of downloading diagnostics configuration file.
corpwifi(config-diag-log)# config

Related Commands

- [*auto-report admin*](#) **on page 886**
- [*auto-report send*](#) **on page 888**
- [*\(diag-log\) admin*](#) **on page 906**
- [*\(diag-log\) restore*](#) **on page 910**
- [*show auto-report-config*](#) **on page 949**

(diag-log) restore

Use this feature only when working with Customer Support. Restores default diagnostics configuration file.

Syntax

restore <filename>

Command Mode

configure terminal > diag-log

Default

NA

Usage

Diagnostics configuration changes can only be done by Fortinet support. If Fortinet support altered a diagnostics configuration file for you, sent it to you, and you implemented it with the command [\(diag-log\) config](#) on [page 908](#), you can return to the default configuration with the command **restore**.

Example

This example restores the default file diag-controller.conf:

```
default# configure terminal
default (config)# diag-log
default (config-diag-log)# restore diag-controller.conf
diag-log restoring diag-controller configuration now...
done
```

This example lists the options for the command:

```
corpwifi# configure terminal
corpwifi(config)# diag-log
corpwifi(config-diag-log)# ?
admin                Manages diagnostics admin status.
config               Download diagnostics configuration file from url.
do                  Executes an IOSCLI command.
end                  Save changes, and return to privileged EXEC mode.
exit                 Save changes, and return to global configuration
mode.
restore              Restores to default diagnostics configuration file.
```

```
corpwifi(config-diag-log)# restore ?
```

```
<file-name>          The file name of restoring default configuration.
```

Related Commands

- [auto-report admin](#) on page 886
- [auto-report send](#) on page 888
- [\(diag-log\) admin](#) on page 906
- [\(diag-log\) config](#) on page 908
- [show auto-report-config](#) on page 949

diagnostics

Collects system diagnostics and outputs to a compressed log file.

Syntax

diagnostics

Command Mode

Privileged EXEC

Default

NA

Usage

The **diagnostics** command gathers system information from the controller and all APs in the WLAN, and places the data into a log file that is compressed then saved. The file can then be sent to Support for debugging system issues. In a WLAN with over 100 APs, this command can take over 10 minutes to complete.

The compressed file name integrates a date stamp that includes the *year.month.day.hour.minutes* (`forti-gather-2007.09.24.20.59.tar.gz`), and is saved in the `images` directory. You can later use the **copy ftp** command to move the file to a server where it can be sent to Support.

Examples

```
controller# diagnostics
Cleaning up previous gather data
Getting process information ...
Getting system log information ...
Getting kernel information ...
Getting network information ...
Getting software information ...
Getting version information ...
Getting disk information ...
Getting Fortinet data ...
Getting high availability information ...
Data gathering phase complete
```

```
images/forti-gather-2007.09.24.20.59.tar.gz created
```

Use the `ftp` option of the `cli` command to move this file off the machine

Related Commands

- [diagnostics-ap](#) on page 914
- [diagnostics-controller](#) on page 916

diagnostics-ap

Collects access point diagnostics for the named AP and outputs to a compressed log file.

Syntax

```
diagnostics-ap all
diagnostics-ap <ap-id>
```

ip-id AP number.

Command Mode

Privileged EXEC

Default

None

Usage

The **diagnostics-ap** command gathers information from the controller and places the data into a log file that is compressed before it is saved. The compressed log file can be sent to Support as an aid in debugging system issues.

The compressed file name integrates a date stamp that includes the *year.month.day.hour.minutes* (*forti-gather-2007.09.24.20.57.tar.gz*), and is saved in the *images* directory. You can later use the **copy ftp** command to move the file to a server where it can be sent to Support.

This command is similar to the **diagnostics** command, but collects only AP information. As such, it will complete in less time than the **diagnostics** command.

Examples

```
controller# diagnostics-ap
Getting process information ...
Getting system log information ...
Getting kernel information ...
Getting network information ...
Getting software information ...
Getting version information ...
Getting disk information ...
Getting Fortinet data ...
Getting high availability information ...
Data gathering phase complete
```

```
images/forti-gather-2007.09.24.20.57.tar.gz created
```

Use the ftp option of the cli command to move this file off the machine

Related Commands

- [diagnostics](#) on page 912
- [diagnostics-controller](#) on page 916

diagnostics-controller

Collects controller diagnostics for the current controller and outputs to a compressed log file.

Syntax

diagnostics-controller

Command Mode

Privileged EXEC

Default

None

Usage

The **diagnostics-controller** command gathers information from the controller, then places the data into a log file that is compressed and saved. This file can then be sent to Support for debugging system issues.

The compressed file name integrates a date stamp that includes the *year.month.day.hour.minutes* (*forti-gather-2007.09.24.20.57.tar.gz*), and is saved in the *images* directory. You can later use the **copy ftp** command to move the file to a server where it can be sent to Support.

This command is similar to the **diagnostics** command, but collects only controller information, so it completes in less time.

Examples

```
controller# diagnostics-controller
Getting process information ...
Getting system log information ...
Getting kernel information ...
Getting network information ...
Getting software information ...
Getting version information ...
Getting disk information ...
Getting Fortinet data ...
Getting high availability information ...
Data gathering phase complete
```

images/forti-gather-2007.09.24.20.57.tar.gz created

Use the **ftp** option of the **cli** command to move this file off the machine

Related Commands

- [diagnostics](#) on page 912
- [diagnostics-ap](#) on page 914

packet-capture-profile

Packet Capture command that either updates an existing profile or creates a new profile and then enters pcap mode.

Syntax

```
packet-capture-profile <profile name>  
no packet capture profile
```

Command Mode

configure terminal > packet-capture-profile

Default

None

Usage

This command either updates an existing packet capture profile or creates a new profile. At the same time, it invokes pcap mode. In pcap mode, you can then use the following packet capture commands:

- Set the list of APs that will send packets with the command [\(packet capture profile\) ap-list on page 921](#).
- Enable the profile (created by the command packet-capture-profile) with the command [\(packet-capture-profile\) enable-profile on page 930](#).
- Set packet truncation length done by APs on the ap-list with the command [\(packet capture profile\) rate-limiting on page 937](#).
- Set rate limiting done by APs on the ap-list with the command [\(packet capture profile\) rate-limiting on page 937](#).
- Determine which packets are sent based on the direction information flows with the command [show auto-report-config on page 949](#). At this time, only rx is available.
- Set the token bucket rate with the command [\(packet capture profile\) token-bucket-rate on page 942](#).
- Set the token bucket size with the command [\(packet capture profile\) token-bucket-size on page 945](#).
- Set the destination for packets with the command [\(packet capture profile\) mode on page 934](#).
- Apply a filter with the command [packet-capture-profile on page 918](#).
- Apply an interface list with the command [\(packet capture profile\) interface list on page 933](#).

The profile created with these commands is downloaded to the APs along with the rest of the NMS configuration download from controller to AP, and the APs start to forward the packets according to the configuration. If you are using Wireshark, you can optionally get a custom Fortinet version from support that recognizes the Fortinet header.

Examples

The following example lists all of the command options, creates the profile LM, sets transmit mode to l3, and sets the ap-list to 16:

```
MC3K-1# configure terminal
MC3K-1(config)# packet-capture-profile ?
ap-list                Set the AP list seperated by commas or all APs.
capture-sibling-frames Enable Capture frames sent by other APs in the net-
work.
enable-profile          Enable this packet capture profile.
end                     Save changes, and return to privileged EXEC mode.
exit mode.              Save changes, and return to global configuration
filter                  Set the filter string.
interface-list          Set the interface list.
mode                    Set the transmit mode to layer2 or layer3.
no                       Delete/reset Pcap profile parameters.
packet-truncation-length Set the packet-truncation-length.
rate-limiting           Enable RateLimiting.
rate-limiting-mode      Set the rate limit per station or cumulative.
rxtx                    Set the traffic snort to tx or rx or both.
token-bucket-rate       Set the token-bucket-rate.
MC3K-1(config)# packet-capture-profile LM
MC3K-1(config-pcap)# mode l3 destination-ip 1.1.1.1 port 9177
MC3K-1(config-pcap)# ap-list 16
MC3K-1(config-pcap)# enable-profile
MC3K-1(config-pcap)# exit
MC3K-1(config)# exit
MC3K-1# show packet-capture-profile LM
AP Packet Capture profiles

Packet Capture Profile Name          : LM
Packet Capture profile Enable/Disable : on
```

```

Modes Allowed L2/L3                : 13
Destination IP Address              : 1.1.1.1
UDP Destination Port                : 9177
Destination MAC for L2 mode         : 00:00:00:00:00:00
Rx only/Tx only/Both               : rx
Rate Limiting per station or cumulative : station
Token Bucket Rate                   : 10
Token Bucket Size                   : 10
AP Selection                        : 16
Extended Filter String              :
Interface List                      :
Packet Truncation Length            : 82
Rate Limiting                       : off
Capture frames sent by other APs in the network : on

```

Related Commands

- [*\(packet capture profile\) ap-list*](#) **on page 921**
- [*\(packet-capture-profile\) enable-profile*](#) **on page 930**
- [*\(packet capture profile\) mode*](#) **on page 934**
- [*\(packet capture profile\) rate-limiting*](#) **on page 937**
- [*\(packet capture profile\) rate-limiting*](#) **on page 937**
- [*\(packet capture profile\) token-bucket-rate*](#) **on page 942**
- [*\(packet capture profile\) token-bucket-size*](#) **on page 945**

(packet capture profile) ap-list

Sets the list of APs from which packets will be forwarded for packet capture.

Syntax

```
ap-list <apid>,<apid>,<apid>  
no ap list
```

apid Comma-separated list of AP IDs from which packets will be forwarded.

Command Mode

configure terminal > packet-capture-profile

Default

None

Usage

This command is used to enter the AP IDs from which the packets are forwarded to a hardware destination in L2/L3 mode as specified in the [\(packet capture profile\) mode on page 934](#) command. This is a subset command in [packet-capture-profile on page 918](#) mode.

Examples

The following example creates the profile LM and designates AP 16 to forward packets:

```
MC3K-1#  
MC3K-1# configure terminal  
MC3K-1(config)# packet-capture-profile LM  
MC3K-1(config-pcap)# mode l3 destination-ip 1.1.1.1 port 9177  
MC3K-1(config-pcap)# ap-list 16  
MC3K-1(config-pcap)# exit  
MC3K-1(config)# exit  
MC3K-1# show packet-capture-profile LM  
AP Packet Capture profiles  
  
Packet Capture Profile Name                                      : LM  
Packet Capture profile Enable/Disable                          : off  
Modes Allowed L2/L3                                               : l3
```

Destination IP Address : 1.1.1.1
UDP Destination Port : 9177
Destination MAC for L2 mode : 00:00:00:00:00:00
Rx only/Tx only/Both : rx
Rate Limiting per station or cumulative : station
Token Bucket Rate : 10
Token Bucket Size : 10
AP Selection : 16
Extended Filter String :
Interface List :
Packet Truncation Length : 82
Rate Limiting : off
Capture frames sent by other APs in the network : on

Related Commands

- [packet-capture-profile](#) **on page 918**
- [\(packet capture profile\) mode](#) **on page 934**

(packet capture profile) capture-sibling-frames

This packet capture command allows frames sent by other AP300/AP200s in the network to be captured.

Syntax

```
capture-sibling-frames
no capture-sibling-frames
```

Command Mode

configuration > packet capture

Default

off

Usage

The command **capture-sibling-frames** allows AP300/AP200s to capture frames sent by other APs. For example, if you did not have a laptop and wanted to know what packets an AP was receiving, you could direct a second AP to listen to packets being sent to its sibling. You could also turn-off (or filter) sibling data for applications such as Location Manager, which improves performance. This command works with and without Virtual Cell, with and without Virtual Port, both on AP200 and AP300.

Examples

This example turns the capture of sibling frames off, then turns it on.

```
default(config)# exit
default# sh packet-capture-profile test
AP Packet Capture profiles
Packet Capture Profile Name           : test
Packet Capture profile Enable/Disable : off
Modes Allowed L2/L3                   : 13
Destination IP Address                 : 0.0.0.0
UDP Destination Port                   : 0
Destination MAC for L2 mode            : 00:00:00:00:00:00
Rx only/Tx only/Both                  : rx
Rate Limiting per station or cumulative : station
Token Bucket Rate                     : 10
Token Bucket Size                     : 10
```

```

AP Selection :
Extended Filter String :
Interface List :
Packet Truncation Length : 82
Rate Limiting : off
Capture frames sent by other APs in the network : on

```

```

default# configure terminal
default(config)# packet-capture-profile test
default(config-pcap)# no capture-sibling-frames
default(config-pcap)# end
default# sh packet-capture-profile test
AP Packet Capture profiles
Packet Capture Profile Name : test
Packet Capture profile Enable/Disable : off
Modes Allowed L2/L3 : L3
Destination IP Address : 0.0.0.0
UDP Destination Port : 0
Destination MAC for L2 mode : 00:00:00:00:00:00
Rx only/Tx only/Both : rx
Rate Limiting per station or cumulative : station
Token Bucket Rate : 10
Token Bucket Size : 10
AP Selection :
Extended Filter String :
Interface List :
Packet Truncation Length : 82
Rate Limiting : off
Capture frames sent by other APs in the network : off

```

This example creates the profile named **test**, turns capture of sibling frames on, and configures capture for Location Manager. Note that the profile has not been enabled yet.

```

default# configure terminal
default(config)# packet-capture-profile test
default(config-pcap)# capture-sibling-frames
default(config-pcap)# end
default# sh packet-capture-profile test

```



```

AP Packet Capture profiles
Packet Capture Profile Name           : test
Packet Capture profile Enable/Disable : off
Modes Allowed L2/L3                   : 13
Destination IP Address                 : 0.0.0.0
UDP Destination Port                   : 0
Destination MAC for L2 mode            : 00:00:00:00:00:00
Rx only/Tx only/Both                  : rx
Rate Limiting per station or cumulative : station
Token Bucket Rate                      : 10
Token Bucket Size                     : 10
AP Selection                           :
Extended Filter String                 :
Interface List                         :
Packet Truncation Length               : 82
Rate Limiting                         : off
Capture frames sent by other APs in the network : on

```

Configuration of Capture Sibling frames field in Packet Capture:

Configuring packet capture profile:

```

-----
Default# configure terminal
Default(config)# packet-capture-profile LM1
Default(config-pcap)# mode 13 destination-ip 172.18.81.11 port 17777
Default(config-pcap)# ap-list 2,3,4,5,6
Default(config-pcap)# enable-profile
Default(config-pcap)# end

```

Controller Output:

```

-----
Default# sh packet-capture-profile LM1
AP Packet Capture profiles

Packet Capture Profile Name           : LM1
Packet Capture profile Enable/Disable : on
Modes Allowed L2/L3                   : 13

```

```

Destination IP Address           : 172.18.81.11
UDP Destination Port             : 17777
Destination MAC for L2 mode      : 00:00:00:00:00:00
Rx only/Tx only/Both            : rx
Rate Limiting per station or cumulative : station
Token Bucket Rate                : 10
Token Bucket Size                : 10
AP Selection                     : 2,3,4,5,6
Extended Filter String           :
Interface List                   :
Packet Truncation Length         : 82
Rate Limiting                   : off
Capture frames sent by other APs in the network : on
Default#

```

AP Output:

ap 2> sniff profile show LM1

```

=====
Name           : LM1
Enabled        : enable
Current State = : Rx
mode           : L3
L2: Destination MAC (L2) : 00:00:00:00:00:00
L3: IP address   : 172.18.81.11
L3: IP port     : 17777
Format         : PPI
Maximum length, truncated: 82
Token bucket rate   : 10
Token bucket size   : 10
Token bucket interval : 100000
Rate limit         : off
Rate limit mode     : station
Filter            : All packets pass
=====
Radio mode        : 1

```

=====

ap 2>

The “capture frames sent by other APs in the network” in the controller output is the option to capture or stop capturing the sibling frames (Fortinet OUI frames). Similarly the filter option in the AP shows what packets to be sent and what to filtered.

This example turns off the capture sibling frames option and enables the profile:

```
Default# configure terminal
Default(config)# packet-capture-profile LM1
Default(config-pcap)# ?
ap-list                Set the AP list seperated by commas.
capture-sibling-frames Enable Capture frames sent by other APs in the net-
work.
enable-profile          Enable this packet capture profile.
end                     Save changes, and return to privileged EXEC mode.
exit mode.              Save changes, and return to global configuration
filter                  Set the filter string.
interface-list          Set the interface list.
mode                    Set the transmit mode to layer2 or layer3.
no                       Delete/reset Pcap profile parameters.
packet-truncation-length Set the packet-truncation-length.
rate-limiting           Enable RateLimiting.
rate-limiting-mode      Set the rate limit per station or cumulative.
rxtx                    Set the traffic snort to tx or rx or both.
token-bucket-rate       Set the token-bucket-rate.
token-bucket-size       Set the token-bucket-size.
Default(config-pcap)# no capture-sibling-frames
Default(config-pcap)# enable-profile
Default(config-pcap)# end
```

Controller output:

```
Default# sh packet-capture-profile LM1
```

AP Packet Capture profiles

```
Packet Capture Profile Name           : LM1
Packet Capture profile Enable/Disable : on
Modes Allowed L2/L3                   : L3
Destination IP Address                 : 172.18.81.11
UDP Destination Port                   : 17777
Destination MAC for L2 mode            : 00:00:00:00:00:00
Rx only/Tx only/Both                  : rx
Rate Limiting per station or cumulative : station
Token Bucket Rate                      : 10
Token Bucket Size                      : 10
AP Selection                           : 2,3,4,5,6
Extended Filter String                 :
Interface List                         :
Packet Truncation Length               : 82
Rate Limiting                         : off
Capture frames sent by other APs in the network : off
Default#
```

AP Output:

ap 2> sniff profile show LM1

=====

```
Name           : LM1
Enabled         : enable
Current State = : Rx
mode           : L3
L2: Destination MAC (L2) : 00:00:00:00:00:00
L3: IP address   : 172.18.81.11
L3: IP port     : 17777
Format          : PPI
Maximum length, truncated: 82
Token bucket rate      : 10
Token bucket size     : 10
Token bucket interval  : 100000
```

```

Rate limit          : off
Rate limit mode     : station
Filter   :
      OUI [ 0: c:e6]
=====

=====

Radio mode          : 1
=====

ap 2>

```

Once this option is turned OFF, the packets with source address 00:0c:e6 (meru) / 00:12:f2 (foundry) and Per Station BSSIDs will not be forwarded by the AP's to the configured server.

Related Commands

- [packet-capture-profile](#) **on page 918**
- [\(packet capture profile\) rate-limiting](#) **on page 937**
- [show packet-capture-profile](#) **on page 959**

(packet-capture-profile) enable-profile

Enables the current capture packet profile.

Syntax

enable-profile
no enable-profile

Command Mode

configure terminal > packet-capture-profile <name>

Default

None

Usage

Use this command to enable or disable packet-capture-profile. This command is a subset command in [\(packet capture profile\) mode](#) **on page 934**.

Examples

This example turns off the capture sibling frames option and then enables the profile:

```
Default# configure terminal
Default(config)# packet-capture-profile LM1
Default(config-pcap)# ?
ap-list                Set the AP list seperated by commas.
capture-sibling-frames Enable Capture frames sent by other APs in the net-
work.
enable-profile          Enable this packet capture profile.
end                    Save changes, and return to privileged EXEC mode.
exit mode.             Save changes, and return to global configuration
filter                 Set the filter string.
interface-list          Set the interface list.
mode                   Set the transmit mode to layer2 or layer3.
no                     Delete/reset Pcap profile parameters.
packet-truncation-length Set the packet-truncation-length.
rate-limiting           Enable RateLimiting.
rate-limiting-mode      Set the rate limit per station or cumulative.
rxtx                   Set the traffic snort to tx or rx or both.
```

```
token-bucket-rate      Set the token-bucket-rate.
token-bucket-size      Set the token-bucket-size.
Default(config-pcap)# no capture-sibling-frames
Default(config-pcap)# enable-profile
Default(config-pcap)# end
```

Related Commands

- [\(packet capture profile\) ap-list](#) on page 921
- [packet-capture-profile](#) on page 918

(packet capture profile) filter

Packet Capture command that sets a MAC address filter for capture. This command is not available at this time.

(packet capture profile) interface list

Packet Capture command that sets an interface list for capture. This command is not available at this time.

(packet capture profile) mode

Packet Capture command that sets the transmit mode to layer2 or layer3 for the current packet capture profile for AP300 and AP200.

Syntax mode 12 destination-mac xx:xx:xx:xx:xx:xx
 mode 13 destination-ip x.x.x.x port <port number>

Command Mode configure terminal > packet-capture-profile

Default None

Usage Two modes can be used for packet capture, L2 and L3. This information is used by the AP when forwarding packets to the destination using either L2 or L3 mode as specified. This is a subset command in [\(packet capture profile\) mode on page 934](#).

Example The following example creates the profile LM and sets transmit mode to l3:

```
MC3K-1# configure terminal
MC3K-1(config)# packet-capture-profile LM
MC3K-1(config-pcap)# mode 13 destination-ip 1.1.1.1 port 9177
MC3K-1(config-pcap)# ap-list 16
MC3K-1(config-pcap)# exit
MC3K-1(config)# exit
MC3K-1# show packet-capture-profile LM
AP Packet Capture profiles
```

```
Packet Capture Profile Name           : LM
Packet Capture profile Enable/Disable : off
Modes Allowed L2/L3                   : l3
Destination IP Address                 : 1.1.1.1
UDP Destination Port                   : 9177
Destination MAC for L2 mode            : 00:00:00:00:00:00
Rx only/Tx only/Both                  : rx
Rate Limiting per station or cumulative : station
```

Token Bucket Rate : 10
Token Bucket Size : 10
AP Selection : 16
Extended Filter String :
Interface List :
Packet Truncation Length : 82
Rate Limiting : off
Capture frames sent by other APs in the network : on

**Related
Commands**

[packet-capture-profile](#) *on page 918*

(packet capture profile) packet-truncation-length

Sets the length of packets that APs forward to a hardware device.

Syntax

`packet-truncation-length <number>`

number Packet length in bytes

Command Mode

configure terminal > packet-capture-profile

Default

None

Usage

This command sets the length of packets that APs forward to a hardware device. APs reduce the length of all packets to this value before forwarding the packet to the hardware destination. Note that for Location manager to work, packets should be at least 82 bytes in length. This is a subset command in [\(packet capture profile\) mode on page 934](#).

Examples

The following command sets packet truncation length to 83:

```
demo# configure terminal
demo(config)# packet-capture-profile MWP
demo(config-pcap)# packet-truncation-length 83
```

Related Commands

[packet-capture-profile on page 918](#)

(packet capture profile) rate-limiting

Packet Capture command that turns rate limiting on and off for the current packet capture profile.

Syntax `rate-limiting`
 `no rate-limiting`

Command Mode `configure terminal > packet-capture-profile`

Default `None`

Usage This command is used to turn on rate limiting. If rate limiting is turned **on**, the rate in the command [\(packet capture profile\) token-bucket-rate on page 942](#) is used to forward the packets. Each AP named by the command [\(packet capture profile\) ap-list on page 921](#) forwards the maximum packets per second configured in the token bucket rate. This is a sub-set command in [packet-capture-profile on page 918](#) mode.

Examples The following example first shows that rate limiting for the packet capture profile is **on** with the **show** command, and then turns rate limiting **off**.

```
default# show packet-capture-profile
Profile Name          L2/L3 Mode      Destination IP  Destination
MAC   Rx/Tx/Both      Rate Limiting  AP Selection
testing                13              0.0.0.0
00:00:00:00:00:00 rx      station
AP Packet Capture profiles(1 entry)
default# configure terminal
default(config)# no packet-capture-profile testing
default(config)# exit
```

- Related Commands**
- [\(packet capture profile\) token-bucket-rate on page 942](#)
 - [\(packet capture profile\) ap-list on page 921](#)
 - [packet-capture-profile on page 918](#)
 - [\(packet capture profile\) token-bucket-rate on page 942](#)

- [\(packet capture profile\) rate-limiting-mode](#) **on page 939**

(packet capture profile) rate-limiting-mode

Packet Capture command that sets the packet capture rate limiting to per-station or cumulative for the current packet capture profile. In this release, the only option is per-station.

Syntax

`rate-limiting station`
`rate-limiting cumulative (not implemented in release 4.0)`

<code>station</code>	Sets rate limiting mode per-station
<code>cumulative</code>	Not functioning for beta test.

Command Mode

Global Configuration

Default

None

Usage

Only **station** is implemented at this time. Rate limiting can be enabled for a packet capture profile using rate limiting command. Rate limiting mode determines whether the limit is per station or AP based on the mode set. If set to **station**, rate limiting is done per station and if set to **AP**, rate limiting is done per AP. The limit based on the Token Bucket Rate and Token Bucket size. Rate determines the number of packets to be forwarded and size determines number of packets that can be cached in memory.

Examples

The following example sets the rate limiting mode to per-station for the packet capture profile named Test.

```
ramecntrl(config)# packet-capture-profile Test
ramecntrl(config-pcap)# rate-limiting-mode station
ramecntrl(config-pcap)# exit
ramecntrl(config)# exit
```

Related Commands

- [\(packet capture profile\) rate-limiting on page 937](#)
- [show packet-capture-profile on page 959](#)

(packet capture profile) rxtx

Sets traffic intrusion detection for the current packet capture profile to received traffic, sent traffic, or both.

Syntax	<code>rxtx rx-only</code> <code>rxtx tx-only</code> <code>rxtx both</code>	
	rx-only	Only traffic being received - only this setting currently works.
	tx-only	Only traffic being sent - this setting is not currently working for beta test
	both	Traffic being sent and received - this setting is not currently working for beta test.

Command Mode Configuration

Default rx-only

Usage Currently sets traffic intrusion detection to monitor received traffic (rx-only). This is a subset command in *(packet capture profile) mode* **on page 934**.

Examples The following command sets traffic intrusion detection to rx only for the packet capture profile named MWP.

```
demo# configure terminal
demo(config)# packet-capture-profile MWP
default(config-pcap)# ?
ap-list           Set the AP list seperated by commas.
capture-sibling-frames Enable Capture frames sent by other APs in the network.
enable-profile     Enable this packet capture profile.
end               Save changes, and return to privileged EXEC mode.
exit              Save changes, and return to global configuration mode.
filter            Set the filter string.
```


interface-list	Set the interface list.
mode	Set the transmit mode to layer2 or layer3.
no	Delete/reset Pcap profile parameters.
packet-truncation-length	Set the packet-truncation-length.
rate-limiting	Enable RateLimiting.
rate-limiting-mode	Set the rate limit per station or cumulative.
rxtx	Set the traffic snort to tx or rx or both.
token-bucket-rate	Set the token-bucket-rate.
token-bucket-size	Set the token-bucket-size.
default(config-pcap)# rxtx ?	
both	Both Rx and Tx
rx-only	Rx only
tx-only	Tx only
demo(config-pcap)# rxtx rx-only	

Related Commands

[packet-capture-profile](#) on page 918

(packet capture profile) token-bucket-rate

Sets the token bucket rate for the current packet capture profile.

Syntax

```
token-bucket-rate <rate>
no token-bucket-rate
```

rate	Number of packets forwarded to the destination at a per-second rate. This is a non-zero value.
------	--

Command Mode

configure terminal > packet-capture-profile

Default

None

Usage

Token-bucket-rate regulates the (non-zero) number of packets forwarded to the destination at a per-second rate if [\(packet capture profile\) rate-limiting on page 937](#) is set to **on**, the token-bucket-rate value tells the APs the maximum number of packets they can forward per second. The token-bucket-rate value should always be lower than [\(packet capture profile\) token-bucket-size on page 945](#) value. If [\(packet capture profile\) rate-limiting on page 937](#) is turned **on**, the number of packets forwarded from an AP is limited to the number of packets set by token-bucket-rate.

Examples

The following example for the packet capture profile named LM sets all possible parameters. Token bucket rate is set to 1000.

```
MC3K-1(config-pcap)#
MC3K-1(config)# packet-capture-profile LM
MC3K-1(config-pcap)# ?
ap-list                Set the AP list seperated by commas.
capture-sibling-frames Enable Capture frames sent by other APs in the net-
work.
enable-profile          Enable this packet capture profile.
end                     Save changes, and return to privileged EXEC mode.
exit                   Save changes, and return to global configuration
mode.
```

```

filter                Set the filter string.
interface-list        Set the interface list.
mode                  Set the transmit mode to layer2 or layer3.
no                     Delete/reset Pcap profile parameters.
packet-truncation-length Set the packet-truncation-length.
rate-limiting          Enable RateLimiting.
rate-limiting-mode     Set the rate limit per station or cumulative.
rxtx                   Set the traffic snort to tx or rx or both.
token-bucket-rate      Set the token-bucket-rate.
token-bucket-size      Set the token-bucket-size.

```

```
MC3K-1(config-pcap)#
```

```
MC3K-1(config-pcap)# tok
```

```
token-bucket-rate token-bucket-size
```

```
MC3K-1(config-pcap)# token-bucket-rate 1000
```

```
MC3K-1(config-pcap)# tok
```

```
token-bucket-rate token-bucket-size
```

```
MC3K-1(config-pcap)# token-bucket-size 10000
```

```
MC3K-1(config-pcap)# mode l3 destination-ip 1.1.1.1 port 17777
```

```
MC3K-1(config-pcap)# rate-limiting
```

```
MC3K-1(config-pcap)# exit
```

```
MC3K-1(config)# exit
```

```
MC3K-1# show packet-capture-profile LM
```

```
AP Packet Capture profiles
```

```
Packet Capture Profile Name           : LM
```

```
Packet Capture profile Enable/Disable : off
```

```
Modes Allowed L2/L3                   : l3
```

```
Destination IP Address                 : 1.1.1.1
```

```
UDP Destination Port                  : 17777
```

```
Destination MAC for L2 mode            : 00:00:00:00:00:00
```

```
Rx only/Tx only/Both                  : rx
```

```
Rate Limiting per station or cumulative : station
```

```
Token Bucket Rate                      : 1000
```

```
Token Bucket Size                      : 10000
```

```
AP Selection                           : 16
```

```
Extended Filter String                 :
```

```
Interface List                         :
```

```
Packet Truncation Length               : 82
```

Rate Limiting : on
Capture frames sent by other APs in the network : on
MC3K-1#

**Related
Commands**

- [\(packet capture profile\) rate-limiting](#) **on page 937**
- [\(packet capture profile\) token-bucket-size](#) **on page 945**

(packet capture profile) token-bucket-size

Sets the depth of the bucket where the wireless packets are stored and then forwarded to the destination.

Syntax

```
token-bucket-size <size>  
no token-bucket-size
```

size	Depth of the bucket where the wireless packets are stored and then forwarded to the destination. This should be a non-zero value and greater than token-bucket-rate.
------	--

Command Mode

configuration mode > packet-capture-profile

Default

None

Usage

Sets the depth of the bucket where the wireless packets are stored and then forwarded to the destination. The [\(packet capture profile\) token-bucket-rate on page 942](#) value should always be lower than token-bucket-size value. If [\(packet capture profile\) rate-limiting on page 937](#) is turned **on**, the packets forwarded from an AP are limited to the number of packets set by [\(packet capture profile\) token-bucket-rate on page 942](#).

Examples

The following example for the packet capture profile named LM sets all possible parameters. Token bucket size is set to 10000.

```
MC3K-1(config-pcap)#  
MC3K-1(config)# packet-capture-profile LM  
MC3K-1(config-pcap)# ?  
ap-list                Set the AP list seperated by commas.  
capture-sibling-frames Enable Capture frames sent by other APs in the network.  
enable-profile          Enable this packet capture profile.  
end                     Save changes, and return to privileged EXEC mode.  
exit                    Save changes, and return to global configuration mode.
```

filter Set the filter string.
 interface-list Set the interface list.
 mode Set the transmit mode to layer2 or layer3.
 no Delete/reset Pcap profile parameters.
 packet-truncation-length Set the packet-truncation-length.
 rate-limiting Enable RateLimiting.
 rate-limiting-mode Set the rate limit per station or cumulative.
 rxtx Set the traffic snort to tx or rx or both.
 token-bucket-rate Set the token-bucket-rate.
 token-bucket-size Set the token-bucket-size.

MC3K-1(config-pcap)#

MC3K-1(config-pcap)# tok

token-bucket-rate token-bucket-size

MC3K-1(config-pcap)# token-bucket-rate 1000

MC3K-1(config-pcap)# tok

token-bucket-rate token-bucket-size

MC3K-1(config-pcap)# token-bucket-size 10000

MC3K-1(config-pcap)# mode l3 destination-ip 1.1.1.1 port 17777

MC3K-1(config-pcap)# rate-limiting

MC3K-1(config-pcap)# exit

MC3K-1(config)# exit

MC3K-1# show packet-capture-profile LM

AP Packet Capture profiles

Packet Capture Profile Name : LM

Packet Capture profile Enable/Disable : off

Modes Allowed L2/L3 : l3

Destination IP Address : 1.1.1.1

UDP Destination Port : 17777

Destination MAC for L2 mode : 00:00:00:00:00:00

Rx only/Tx only/Both : rx

Rate Limiting per station or cumulative : station

Token Bucket Rate : 1000

Token Bucket Size : 10000

AP Selection : 16

Extended Filter String :

Interface List :

Packet Truncation Length : 82

Rate Limiting : on
Capture frames sent by other APs in the network : on
MC3K-1#

**Related
Commands**

- [\(packet capture profile\) rate-limiting](#) **on page 937**
- [\(packet capture profile\) token-bucket-rate](#) **on page 942**

remote-log

Configure a remote site for maintaining logs.

Syntax

```
remote-log start smb <mount-point> <workgroup> <username>  
remote-log stop smb <mount-point> <workgroup> <username>
```

<i>mount-point</i>	Specifies the mount point of the remote disk (<i>//hostname/sharename</i>).
<i>workgroup</i>	Specifies the workgroup where the user has permission to create remote log configuration.
<i>username</i>	Specifies the name of the user creating the remote log configuration.

Command Mode

Privileged EXEC

Default

None

Usage

The **remote-log** command allows you to copy all system logs to a network shared disk. By default, log entries are stored on the controller flash card, which by its nature is limited. As a result, log entries are purged when a certain amount of space is consumed to allow for newer entries. By specifying a network share, the complete history of logged entries can be kept.

To establish remote logging, use the command **remote-log start smb** and add an optional network mount-point, workgroup, and username. You will be prompted for the username password. To stop the remote logging and unmount the share, use the same command parameters but use the **stop** keyword instead of the **start** keyword.

Be sure you have a reliable connection to the share. You will be prompted for your workgroup and username, if it is not supplied on the command line.

Examples

The following commands allow the user admin in the engineering workgroup to create a remote log on the server maple using the shared disk IT:

```
controller# remote-log start smb //maple/IT engineering admin  
controller#
```


show auto-report-config

Lists the auto-reporting configuration created by the auto-report commands **send** and **admin**.

Syntax

show auto-report-config

Command Mode

Configuration mode > Auto-report mode

Default

none

Usage

Use this command to see the configured values used in auto-reporting.

Examples

This example sends a report to `cwon:cwon@172.27.0.79/diagagent.conf` every hour. Look at the last command to see the **show auto-report-config** command:

```
default#configure terminal
default(config)# auto-report
default(config-auto-report)# ?
```

```
adminConfigures administration mode for auto-reporting
do Executes an IOSCLI command
endSaves changes and returns to privileged exec mode
exitSaves changes and returns to global configuration mode
sendUploads log files to named URL once or periodically
```

```
default(config-auto-report)# send ftp://cwon:cwon@172.27.0.79/diag-
gent.conf 1
default(config-auto-report)# admin on
default(config-auto-report)# show auto-report-config
```

```
Administration Statuson
Auto-reporting Intervalevery hour
Auto-reporting URLcwon:cwon@172.27.0.79
```

Related Commands

- [auto-report admin](#) on page 886
- [auto-report send](#) on page 888
- [\(diag-log\) admin](#) on page 906
- [\(diag-log\) config](#) on page 908
- [\(diag-log\) restore](#) on page 910

show cef

Lists ArcSight's Common Event Format (CEF) logging.

Syntax

show auto-report config

Command Mode

EXEC mode

Default

none

Usage

Use this command to see the configured values used for CEF logging.

Examples

This example lists CEF logging options and then shows the current CEF settings.

```
BangWiFi36# configure terminal
BangWiFi36(config)# cef ?
disable           Disables Common Event Format Logging Feature.
enable            Enables Common Event Format Logging Feature.
server-ip         Enter Server Details
BangWiFi36(config)# exit
BangWiFi36#
BangWiFi36# show cef
CEF Logging is disabled
CEF Logging Host is not configured
BangWiFi36#
```

show debug

Displays debug information.

Syntax

show debug

Command Mode

Privileged EXEC

Default

NA

Usage

Use this command to display debug information.

Example

```
ramecntrl# show debug
Current trace status:
  Current log entries      : 920 (Out of 10000 max.)
  Log frozen?             : NO
  Auto-freeze severity    : -1 (Disabled)
  Real-time display severity : -1 (Disabled)
ramecntrl#
```

show diag-log-config ap/controller/station

Displays the diagnostic logging configurations for APs, controllers, and stations.

Syntax

```
show diag-log-config ap
show diag-log-config controller
show diag-log-config station
```

Command Mode

Privileged EXEC

Default

Disabled

Usage

This command is used to view the administrative status and Diagnostics Logging configuration of controller, ap and station diagnostics. This Events parameter was added to **show diag-log-config station** in release 4.0.

Examples

This example shows all of the controller thresholds for diagnostic inferences.

```
ramecntrl# sh diag-log-config ap
```

```
AP Diagnostics                      Disabled
AP Diag Stats Monitoring Interval    240 seconds
AP interface Stats Monitoring Interval 300 seconds
```

Diagnostics Type	SubType	Debug	Infor	Minor	Major
Fatal Hw Error Interrupts 2	diag stats	-	-	-	1
Rx Overrun Interrupts 2	diag stats	-	-	-	1
Rx eol Interrupts 2	diag stats	-	-	-	1
Tx Underrun Interrupts 2	diag stats	-	-	-	1

Tx Timeout Interrupts 1260	diag stats	-	-	-	1200
Carrier Sense Timeout Int 1260	diag stats	-	-	-	1200
Tx Failed(No Tx Buff) 2	diag stats	-	-	-	1
Tx Failed(Fifo Underrun) 2	diag stats	-	-	-	1
No SkBuff for Beacon 2	diag stats	-	-	-	1
Aggregate Desc Conf Err 2	diag stats	-	-	-	1
Data Underrun Aggregate 2	diag stats	-	-	-	1
Delimiter Underrun Aggregate 2	diag stats	-	-	-	1
Rx pkts with Bad Version 2	diag stats	-	-	-	1
Beacon Misscount -	diag stats	-	-	-	-
Beacon buff Null Cnt 2	diag stats	-	-	-	1
Radio Reset(Beacon Stuck) 21	diag stats	-	-	-	20
Radio Reset(TP Scale) 2	diag stats	-	-	-	1
Radio Reset(Fatal Tasklet) 2	diag stats	-	-	-	1
Radio Reset(Rx Overrun Tasklet) 2	diag stats	-	-	-	1
Radio Reset(Calibrate) 2	diag stats	-	-	-	1
Radio Reset(Tx Ant Switch) 2	diag stats	-	-	-	1
Radio Reset(Rx Chain) 2	diag stats	-	-	-	1
Radio Reset(No Tx Frames) 2	diag stats	-	-	-	1
Radio Reset(Total) 2	diag stats	-	-	-	1
Tid Reset Count 2	diag stats	-	-	-	1

Slam Tx No Ack Addr	diag stats	-	-	-	3000
-					
Tx Failed(Too Many Retries)	if stats	-	-	-	120000
-					
Tx Excessive Retries Aggre	if stats	-	-	-	120000
-					
Rx Data for Assigned sta	if stats	-	-	-	-
-					
All Tx Frames	if stats	-	-	-	-
-					
Rx Mgmt for Assigned sta	if stats	-	-	-	12000
-					
Rx All Data Frames	if stats	-	-	-	-
-					
Rx All Mgmt Frames	if stats	-	-	-	120000
-					
Rx All Cntl Frames	if stats	-	-	-	240000
-					
Mgmt Frames Overhead in Airtime	if stats	-	-	-	30
-					
Association Count	if stats	-	-	-	40
-					
Retry Percentage	if stats	-	-	-	40
-					
Noise Floor	if stats	-	-	-	-75
-					

namecntrl# sh diag-log-config controller

Controller Diagnostics	Disabled
Monitoring Interval	60 second(s)

Diagnostics Type	SubType	Object-ID	Debug	Infor	Minor
Major	Critical				
process-restart	crash	-	-	-	-
ON					
process-resource	mem-usage(%)	-	-	50	70
90					
process-resource	cpu-usage(%)	-	-	50	70
90					

keepalive-timeout 9	all(N)		-	-	5	7
cpu-usage 90	process(%)		-	-	50	70
file-system 90	all(%)		-	-	50	70
file-system -	partition(%)	0	-	-	-	-
partition 1000	access(N/sec)		-	-	100	500
mem-usage 200	free-mem(MB)		-	-	-	-
mailbox ON	all		-	-	-	-
mailbox -	mailbox	0	-	-	-	-
wncreg-table -	state		-	ON	-	-
ats-table ON	state		-	-	-	-
interface 100	error(N)		-	-	10	50
client-density 100	all(%)		-	-	80	90
ip-conflict ON	all		-	-	-	-
ip-unassigned -	all		-	-	-	-
gateway-unreach ON	error		-	-	-	-
radius-svr-unreach ON	error		-	-	-	-
dhcp-svr-unreach ON	error		-	-	-	-

```
ramecntrl# sh diag-log-config station
```

Station Diagnostics	Disabled
Station Diagnostics Data Collection Interval	60 second(s)
State Diagnostics Inference Interval	300 second(s)

Inference Threshold Table

Station Counter	ID#	Low	High
MAC Filter ACL Success	1	-	5
MAC Filter ACL Failure	2	-	5
Radius Auth Success	3	-	5
Radius Auth Failure	4	-	5
Assignment Failure	5	-	5
Association Success	6	-	5
Key Exchange Success	7	-	5
Key Exchange Failure	8	-	5
MIC Failure	9	-	5
IP Address Update	10	-	10
Data Decryption Failure	11	-	5
CP Guest User Success	12	-	5
CP Guest User Failure	13	-	5
Soft Handoff	14	-	15

Inference Rule Table

ID#	Inference Description	Severity	Operational Counter ID#
1	MAC Filtering ACL Failure	Critical	2
2	Radius Authentication Failure	Critical	4
3	Assignment Failure	Critical	5
4	Association Success	Infor	6
5	802.1x Key Exchange Failure	Critical	8
6	MIC Failure	Critical	9
7	IP Address Update	Infor	10
8	Data Decryption Failure	Critical	11
9	CP Guest User Failure	Critical	13
10	Soft-Handoff	Infor	14
11	Hard-Handoff	Infor	6 & 10

namecntrl#

Related Commands

- [\(diag-log\) admin](#) **on page 906**
- [\(diag-log\) config](#) **on page 908**
- [\(diag-log\) restore](#) **on page 910**
- admin ap on
- admin controller on
- admin station on

show packet-capture-profile

Displays all packet capture profiles along with their state and mode. Optionally, displays one named packet capture profile.

Syntax

```
show packet-capture-profile
show packet-capture-profile <profile name>
```

profile name Changes the command to show only the named profile

Command Mode

EXEC mode

Default

All packet capture profiles

Usage

The command with no profile name displays all packet capture profiles along with their state (enabled/disabled) and mode (layer 2/layer 3). This command also displays that information for a single named packet capture profile.

Examples

The following example shows the profile LM, but now the profile is disabled:

```
MMC3K-1# show packet-capture-profile LM
AP Packet Capture profiles
Packet Capture Profile Name           : LM
Packet Capture profile Enable/Disable : off
Modes Allowed L2/L3                   : 13
Destination IP Address                 : 1.1.1.1
UDP Destination Port                   : 9177
Destination MAC for L2 mode            : 00:00:00:00:00:00
Rx only/Tx only/Both                  : rx
Rate Limiting per station or cumulative : station
Token Bucket Rate                      : 10
Token Bucket Size                      : 10
AP Selection                           : 16
Extended Filter String                 :
Interface List                         :
```

```

Packet Truncation Length          : 82
Rate Limiting                     : off
Capture frames sent by other APs in the network : on
This example shows the status of the profile called Test:
corporatewifi# show packet-capture-profile test
AP Packet Capture profiles:
Packet Capture Profile Name       : test
Packet Capture profile Enable/Disable : on
Modes Allowed L2/L3               : l3
Destination IP Address            : 192.168.34.210
UDP Destination Port              : 9178
Destination MAC for L2 mode       : 00:00:00:00:00:00
Rx only/Tx only/Both             : rx
Rate Limiting per station or cumulative : station
Token Bucket Rate                 : 10
Token Bucket Size                 : 10
AP Selection                      : all
Extended Filter String            :
Interface List                    :
Packet Truncation Length          : 0
Rate Limiting                     : off
Capture frames sent by other APs in the network : on

```

Related Commands

[packet-capture-profile](#) on page 918

show statistics AP300-diagnostics

Displays the list of AP300 diagnostics statistics per interface.

Syntax `show statistics ap300-diagnostics`

Command Mode Privileged EXEC mode

Default NA

Usage

Example This example shows the results of the command `show statistics AP300-diagnostics`.

Master1# `show statistics ap300-diagnostics`

AP-ID	IfIndex	AP-Name	Fatal	HW	INT	Tx	Underrun	INT	Tx	Timeout	INT
Carrier	Sense	Timeout	Rx	Overrun	INT	Rx	EOL	INT			
3	1	3-Guha	0	0		321	0				
48		0									
3	2	3-Guha	0	0		213	0				
306		0									
4	1	4-QA.Facing	0	0		3446	0				
0		0									
4	2	4-QA.Facing	0	0		6689	0				
0		0									
5	1	5-Popov	0	0		687	0				
251		0									
5	2	5-Popov	0	0		322	0				
788		0									
8	1	8-Amazon	0	0		374119	0				
0		0									
8	2	8-Amazon	0	0		14	0				
0		0									
96	1	AP-96	0	0		1775	0				
12		0									

96	2	AP-96	0	0	0	0
0		1				
98	1	9-GrndConf	0	0	3764	0
0		0				
98	2	9-GrndConf	0	0	0	0
0		0				
103	1	103-carlos	0	0	467	0
24		0				
103	2	103-carlos	0	0	356	0
412		1				
239	1	AP-239	0	0	7492	0
0		0				
239	2	AP-239	0	0	2	0
2		0				

AP300 Diagnostic Statistics(16 entries)

Master1#

**Related
Commands**

[diagnostics](#) on page 912